



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08185448 A**(43) Date of publication of application: **16.07.96**

(51) Int. Cl. **G06F 17/60**
G06F 15/00
G09C 1/00
H04L 9/00
H04L 9/10
H04L 9/12

(21) Application number: **07228366**(22) Date of filing: **05.09.95**

(30) Priority: **30.09.94 JP 06237673**
27.10.94 JP 06264199
02.11.94 JP 06269959

(71) Applicant: **MITSUBISHI CORP**

(72) Inventor: **SAITO MAKOTO**
MOMIKI JIYUNICHI

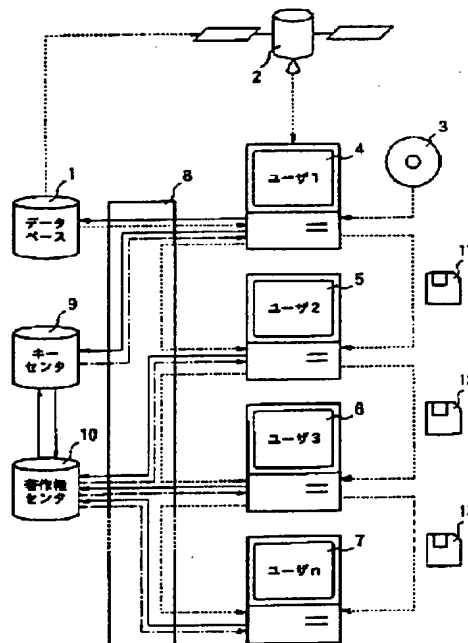
(54) **SYSTEM AND DEVICE FOR MANAGING DATA COPYRIGHT**

(57) Abstract:

PURPOSE: To provide a data copyright managing system in a multi-media system.

CONSTITUTION: Data supplied from a data base 1 to users 4-9 are ciphered and distributed and the user deciphers the ciphered data by using a cryptographic key obtained from a key managing center 9 or a copyright managing center 10 and utilizes them. When preserving, copying or transferring the data by the users 4-9, though the data are ciphered again, this cryptographic key is supplied from the key managing center 9 or the copyright managing center 10 or generated by a copyright managing program.

COPYRIGHT: (C)1996,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-185448

(43) 公開日 平成8年(1996)7月16日

(51) Int.Cl. ⁴	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 17/80				
15/00	3 9 0	9364-5L		
G 0 9 C 1/00		7259-5J		
			G 0 6 F 15/ 21	Z
			H 0 4 L 9/ 00	Z

審査請求 未請求 請求項の数48 O L (全 36 頁) 最終頁に続く

(21) 出願番号 特願平7-228368

(22) 出願日 平成7年(1995)9月5日

(31) 優先権主張番号 特願平6-237673

(32) 優先日 平6(1994)9月30日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平6-264199

(32) 優先日 平6(1994)10月27日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平6-269959

(32) 優先日 平6(1994)11月2日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005979

三菱商事株式会社

東京都千代田区丸の内2丁目6番3号

(72) 発明者 斉藤 誠

東京都千代田区丸の内2丁目6番3号 三

菱商事株式会社内

(72) 発明者 初木 単一

東京都千代田区丸の内2丁目6番3号 三

菱商事株式会社内

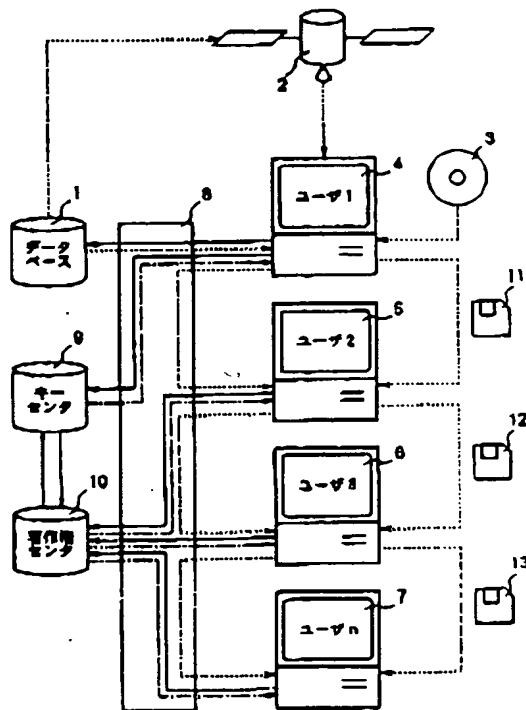
(74) 代理人 弁理士 南條 眞一郎

(54) 【発明の名称】 データ著作権管理システム及びデータ著作権管理装置

(57) 【要約】 (修正有)

【課題】 マルチメディアシステムに於けるデータ著作権、管理システムを提供する。

【解決手段】 データベース1からユーザ4~9に供給されるデータは暗号化して配布され、ユーザは鍵管理センタ9あるいは著作権管理センタ10から入手した暗号鍵を用いて暗号化データを復号化して利用する。ユーザ4~9がデータを保存、複写あるいは転送する場合にデータは再暗号化されるが、この鍵は鍵管理センタ9あるいは著作権管理センタ10から供給されるか著作権管理プログラムによって生成される。



【特許請求の範囲】

【請求項1】 暗号化されてデータベースから利用者に供給されるデータの著作権を管理するデータ著作権管理システムであって：該データ著作権管理システムは、データベース1及び鍵管理センタ9を有し；前記暗号化データの復号鍵が前記鍵管理センタ9から前記利用者に供給され；前記利用者が前記データを表示あるいは加工を行う場合には前記復号鍵を用いて前記暗号化データが復号され；前記利用者が前記データあるいは前記加工が行われたデータを保存、複写あるいは転送する場合には前記データが再暗号化される、データ著作権管理システム。

【請求項2】 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、請求項1記載のデータ著作権管理システム。

【請求項3】 前記著作権管理プログラムが前記利用者が使用する装置のROMに格納されている、請求項3記載のデータ著作権管理システム。

【請求項4】 前記著作権管理プログラムが前記利用者が使用する装置のオペレーティングシステムが管理するシステム領域に格納されている、請求項3記載のデータ著作権管理システム。

【請求項5】 さらに、前記データの著作権を管理する著作権管理プログラムが用いられる、請求項1又は請求項2記載のデータ著作権管理システム。

【請求項6】 さらに、前記データの著作権についての暗号化されていない著作権情報が用いられる、請求項1、請求項2、請求項3、請求項4又は請求項5記載のデータ著作権管理システム。

【請求項7】 前記暗号化されていない著作権情報が著作権情報ラベルとして前記暗号化データに付加されており、前記データの保存、複写あるいは転送が行われた場合に前記著作権情報ラベルが前記データとともに保存、複写あるいは転送される、請求項1、請求項2、請求項3、請求項4、請求項5又は請求項6記載のデータ著作権管理システム。

【請求項8】 前記著作権情報ラベルにデジタル署名がされている、請求項7記載のデータ著作権管理システム。

【請求項9】 データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース、1鍵管理センタ9及び著作権管理センタ10から構成され；前記データ著作権管理システムでは秘密鍵、利用者情報及び著作権管理プログラムが利用され；前記データベース1はデータを第1秘密鍵によって暗号化して通信ネットワーク8、通信・放送衛星2、記録媒体3を介して1次ユーザ4に配布し；前記1次ユーザ4は前記鍵管理センタ9に対して1次ユーザ情報を提示して利用要求を行い；前記鍵管理センタ9は前記1次

ユーザ情報を前記著作権管理センタ10に転送し；前記鍵管理センタ9は前記第1秘密鍵及び第2秘密鍵とともに著作権管理プログラムを前記通信ネットワーク8を経由して前記1次ユーザ4に転送し；前記1次ユーザ4は前記著作権管理プログラムにより前記第1秘密鍵を用いて前記暗号化データを復号化して利用し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第2秘密鍵を用いて再暗号化されるとともにコピーあるいは転送される再暗号化データに暗号化されていない1次ユーザ情報が付加される、データ著作権管理システム。

【請求項10】 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第1秘密鍵及び第2秘密鍵が廃棄され；前記暗号化データを再利用する前記1次ユーザ4は前記著作権管理センタ10に再暗号化データの再利用のために前記第2秘密鍵の再転送を申し込み；前記第2秘密鍵が再転送される、請求項9記載のデータ著作権管理システム。

【請求項11】 前記第2秘密鍵が再転送されたことにより、前記著作権管理センタ10に前記暗号化データのコピーあるいは転送が登録される、請求項10記載のデータ著作権管理システム。

【請求項12】 2次ユーザ5は前記著作権管理センタ10に前記1次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ10は前記1次ユーザ4に対する前記第2秘密鍵の再転送を確認した上で前記2次ユーザ5に前記第2秘密鍵及び第3秘密鍵及び前記著作権管理プログラムを転送し；前記2次ユーザ5は前記著作権管理プログラムにより前記第2秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第3秘密鍵を用いて再暗号化及び再復号化が行われる、請求項10又は請求項11記載のデータ著作権管理システム。

【請求項13】 前記第2秘密鍵が前記著作権管理プログラムにより前記第1秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか1つあるいはいくつかに基づいて生成される、請求項9、請求項10、請求項11又は請求項12記載のデータ著作権管理システム。

【請求項14】 データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース1、鍵管理センタ9及び著作権管理センタ10から構成され；前記データ著作権管理システムでは秘密鍵、利用者情報及び著作権管理プログラムが利用され；1次ユーザ4は前記データベース1に1次ユーザ4情報を提示してデータの利用要求を行い；前記データベース1は要求された前記データを第1秘密鍵を用いて暗号化して前記第1秘密鍵、前記第2秘密鍵及び前記著

10

20

30

40

50

著作権管理プログラムとともに前記通信ネットワーク 8 を経由して前記 1 次ユーザ 4 に転送し；前記鍵管理センタ 9 は前記 1 次ユーザ情報を前記著作権管理センタ 10 に転送し；前記鍵管理センタ 9 は前記第 1 秘密鍵及び第 2 秘密鍵とともに著作権管理プログラムを前記通信ネットワーク 8 を経由して前記 1 次ユーザ 4 に転送し；前記 1 次ユーザ 4 は前記著作権管理プログラムにより前記第 1 秘密鍵を用いて前記暗号化データを復号化して利用し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第 2 秘密鍵を用いて再暗号化されるとともにコピーあるいは転送される再暗号化データに暗号化されていない 1 次ユーザ情報が付加される、データ著作権管理システム。

【請求項 15】 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第 1 秘密鍵及び第 2 秘密鍵が廃棄され；前記暗号化データを再利用する場合には前記 1 次ユーザ 4 は前記著作権管理センタ 10 に再暗号化データの再利用のために前記第 2 秘密鍵の再転送を申し込み；前記第 2 秘密鍵が再転送される、請求項 14 記載のデータ著作権管理システム。

【請求項 16】 前記第 2 秘密鍵が再転送されたことにより、前記著作権管理センタ 10 に前記暗号化データのコピーあるいは転送が登録される、請求項 15 記載のデータ著作権管理システム。

【請求項 17】 前記 2 次ユーザ 5 は前記著作権管理センタ 10 に前記 1 次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ 10 は前記 1 次ユーザ 4 への前記第 2 秘密鍵の再転送を確認した上で前記 2 次ユーザ 5 に前記第 2 秘密鍵及び第 3 秘密鍵及び前記著作権管理プログラムを転送し；前記 2 次ユーザ 5 は前記著作権管理プログラムにより前記第 2 秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第 3 秘密鍵を用いて再暗号化及び再復号化が行われる、請求項 15 又は請求項 16 記載のデータ著作権管理システム。

【請求項 18】 前記第 2 秘密鍵が前記著作権管理プログラムにより前記第 1 秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか 1 つあるいはいくつかに基づいて生成される、請求項 14、請求項 15、請求項 16 又は請求項 17 記載のデータ著作権管理システム。

【請求項 19】 データベースから利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：前記データ著作権管理システムはデータベース 1、鍵管理センタ 9 及び著作権管理センタ 10 から構成され；前記データ著作権管理システムでは秘密鍵、公開鍵及び専用鍵が利用され；1 次ユーザ 4 は前記鍵管理センタ 9 に前記第 1 公開鍵、第 2 公開鍵及び 1

次ユーザ情報を提示して利用希望データの利用要求を行い；利用要求を受けた前記データベース 1 は前記データを前記第 1 秘密鍵を用いて暗号化し、

前記第 1 秘密鍵を前記第 1 公開鍵を用いて暗号化し、前記第 2 秘密鍵を前記第 2 公開鍵を用いて暗号化し、前記暗号化データ、前記暗号化第 1 秘密鍵及び前記暗号化第 2 秘密鍵及び著作権管理プログラムを前記 1 次ユーザ 4 に転送し；前記 1 次ユーザ 4 は著作権管理プログラムにより前記暗号化第 1 秘密鍵を前記第 1 専用鍵を用いて復号化し、

前記暗号化データを前記復号化第 1 秘密鍵を用いて復号化し、

前記暗号化第 2 秘密鍵を前記第 2 専用鍵を用いて復号化し、

前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第 2 秘密鍵を用いて暗号化及び復号化が行われる、データ著作権管理システム。

【請求項 20】 前記復号化データがコピーあるいは転送されたときには前記著作権管理プログラムにより前記第 1 秘密鍵及び第 2 秘密鍵が廃棄され；前記暗号化データを再利用する前記 1 次ユーザ 4 は前記著作権管理センタ 10 に再暗号化データの再利用のために前記第 2 秘密鍵の再転送を申し込み；前記第 2 秘密鍵が再転送される、

請求項 19 記載のデータ著作権管理システム。

【請求項 21】 前記第 2 秘密鍵が再転送されたことにより、前記著作権管理センタ 10 に前記暗号化データのコピーあるいは転送が登録される、請求項 20 記載のデータ著作権管理システム。

【請求項 22】 前記 2 次ユーザ 5 は前記著作権管理センタ 10 に前記 1 次ユーザ情報を提示して利用要求を行い；前記著作権管理センタ 10 は前記 1 次ユーザ 4 に対する前記第 2 秘密鍵の再転送を確認した上で前記 2 次ユーザ 5 に前記第 2 秘密鍵及び第 3 秘密鍵及び前記著作権管理プログラムを転送し；前記 2 次ユーザ 5 は前記著作権管理プログラムにより前記第 2 秘密鍵を用いて前記暗号化データを復号化し；前記復号化データの保存、コピーあるいは転送が行われる場合には前記著作権管理プログラムにより前記第 3 秘密鍵を用いて再暗号化及び再復号化が行われる、請求項 20 又は請求項 21 記載のデータ著作権管理システム。

【請求項 23】 前記第 2 秘密鍵が前記著作権管理プログラムにより前記第 1 秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか 1 つあるいはいくつかに基づいて生成される、請求項 19、請求項 20、請求項 21 又は請求項 22 記載のデータ著作権管理システム。

【請求項 24】 各々異なる暗号鍵で暗号化されてデータベース 1 から利用者に供給される複数のデータを利用

10

20

30

40

50

するためのデータ著作権管理システムであって：該データ著作権管理システムでは暗号鍵、利用者情報及び著作権管理プログラムが利用され；1次ユーザ4は著作権管理センタ10から前記複数の原データ固有の複数の著作権管理プログラム及び複数の第1暗号鍵を入手し、前記複数の原データを前記複数の第1暗号鍵で復号し；前記複数の原データ固有の複数の著作権管理プログラムにより1つ又は複数の第2暗号鍵が生成され；利用された前記複数の原データあるいは複数の加工データは前記複数の原データ固有の複数の著作権管理プログラムにより前記1つ又は複数の第2暗号鍵で暗号化されて加工過程データとともに保存・複写・転送され；前記1つ又は複数の第2の暗号鍵で暗号化された前記複数の原データあるいは前記複数の加工データは2次ユーザ5が前記著作権管理センタ10から入手した前記複数の著作権管理プログラム及び前記1つ又は複数の第2の暗号鍵で復号化されて前記加工過程データを用いて加工されて利用される、データ著作権管理システム。

【請求項25】 前記第2秘密鍵が前記著作権管理プログラムにより前記第1秘密鍵、前記ユーザ情報、前記著作権管理プログラムの使用回数のいずれか1つあるいはいくつかに基づいて生成される、請求項24記載のデータ著作権管理システム。

【請求項26】 データベース1から利用者に暗号化されて供給されるデータを利用するためのデータ著作権管理システムであって：該データ著作権管理システムでは暗号鍵、利用者情報及び著作権管理プログラムが利用され；前記利用者は前記データベース1に利用者情報を提示し；前記データベース1は前記第1利用者に第1暗号鍵で暗号化された前記データを供給し；前記第1利用者は前記著作権管理プログラムを利用して前記第1暗号鍵に基づく第2暗号鍵を生成し；前記第1利用者が前記暗号化データを利用する場合には前記第1暗号鍵を用いて前記暗号化データが復号され；前記第1利用者が前記復号化データを保存、複写あるいは転送する場合には、前記復号化データが前記第2暗号鍵を用いて再暗号化される、データ著作権管理システム。

【請求項27】 前記暗号鍵が秘密鍵である、請求項26記載のデータ著作権管理システム。

【請求項28】 前記暗号鍵が公開鍵及び専用鍵である、請求項26記載のデータ著作権管理システム。

【請求項29】 暗号化されて金融機関から第1利用者に供給されるデジタルキャッシュを利用するためのデジタルキャッシュ管理システムであって：該デジタルキャッシュ管理システムにおいては、前記暗号化デジタルキャッシュデータの復号鍵が金融機関から前記第1利用者に供給され；前記第1利用者が前記デジタルキャッシュデータの確認を行う場合には前記復号鍵を用いて前記暗号化デジタルキャッシュデータが復号され；前記第1利用者が前記復号化デジタルキャッシュ

データを保存する場合、変更されたデジタルキャッシュデータを保存する場合、あるいは第2利用者にデジタルキャッシュデータを転送する場合には前記データが再暗号化される、デジタルキャッシュ管理システム。

【請求項30】 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、請求項29のデジタルキャッシュ管理システム。

【請求項31】 さらに、前記デジタルキャッシュを管理するデジタルキャッシュ管理プログラムが用いられる、請求項29又は請求項30のデジタルキャッシュ管理システム。

【請求項32】 さらに、暗号化されていない第1利用者情報が用いられる、請求項29、請求項30又は請求項31のデジタルキャッシュ管理システム。

【請求項33】 前記暗号化されていない第1利用者情報が第1利用者情報ラベルとして前記暗号化デジタルキャッシュデータに付加されており、前記デジタルキャッシュデータが保存される場合、変更されたデジタルキャッシュデータが保存される場合、あるいは第2利用者にデジタルキャッシュデータが転送される場合には前記デジタルキャッシュデータとともに保存あるいは転送される、請求項29、請求項30、請求項31又は請求項32のデジタルキャッシュ管理システム。

【請求項34】 前記第1利用者情報ラベルにデジタル署名がされている、請求項33記載のデータ著作権管理システム。

【請求項35】 暗号化されて金融機関から第1利用者に供給されるデジタルキャッシュを利用するためのデジタルキャッシュ管理システムであって：該デジタルキャッシュ管理システムでは暗号鍵、利用者情報及びデジタルキャッシュ管理プログラムが利用され；前記第1利用者は前記金融機関に第1利用者情報を提示し；前記金融機関は前記第1利用者に第1暗号鍵で暗号化された前記デジタルキャッシュを供給し；前記第1利用者は前記デジタルキャッシュ管理プログラムを利用して前記第1暗号鍵に基づく第2暗号鍵を生成し；前記第1利用者が前記暗号化デジタルキャッシュデータの確認を行う場合には前記第1暗号鍵を用いて前記暗号化デジタルキャッシュデータが復号され；前記利用者が前記復号化デジタルキャッシュデータを保存する場合には、前記第2暗号鍵を用いて再暗号化され；前記復号化デジタルキャッシュデータが第2利用者に転送される時に前記第2暗号鍵を用いて再暗号化され、前記再暗号化デジタルキャッシュデータが前記第1利用者情報とともに前記第2利用者に転送され；前記第2利用者から前記金融機関に前記第1利用者情報が提示され；前記金融機関は前記第1利用者情報に基づく前記第2暗号鍵を生成して前記第2利用者に転送し；前記第2利用者は前記転送された第2暗号鍵を用いて前記デジタルキャッシュ管理プログラムにより前記再暗号化デジタルキャ

ッシュデータを復号する、デジタルキャッシュ管理システム。

【請求項36】 前記暗号鍵が秘密鍵である、請求項35のデジタルキャッシュ管理システム。

【請求項37】 前記暗号鍵が公開鍵及び専用鍵である、請求項35のデジタルキャッシュ管理システム。

【請求項38】 暗号化されて金融機関から第1利用者に供給されるデジタルキャッシュを利用するためのデジタルキャッシュ管理システムであって：該デジタルキャッシュ管理システムでは公開鍵及び専用鍵が利用され；前記第1利用者は前記金融機関に第1公開鍵を提示し；前記金融機関は前記第1公開鍵でデジタルキャッシュデータを暗号化して前記第1利用者に供給し；前記第1利用者は前記デジタルキャッシュデータを第1専用鍵を用いて復号し；前記第2利用者は前記第1利用者に第2公開鍵を提示し；前記第1利用者は復号化された前記デジタルキャッシュデータを第2公開鍵で暗号化して第2利用者に転送し；前記第2利用者は前記デジタルキャッシュデータを第2専用鍵を用いて復号する、デジタルキャッシュ管理システム。

【請求項39】 第1利用者から第2利用者に暗号化されて供給されるテレビジョン会議データを利用するためのテレビジョン会議データ管理システムであって：該テレビジョン会議データ管理システムにおいては、前記暗号化テレビジョン会議データの復号鍵が第1利用者から前記第2利用者に供給され；前記第2利用者が前記テレビジョン会議データを利用する場合には前記復号鍵を用いて前記暗号化テレビジョン会議データが復号され；前記第2利用者が前記復号化テレビジョン会議データを保存する場合、加工されたテレビジョン会議データを保存する場合、あるいは第3利用者にテレビジョン会議データを転送する場合には前記データが再暗号化される、テレビジョン会議データ管理システム。

【請求項40】 前記再暗号化に用いられる暗号鍵が前記復号鍵とは異なる暗号鍵である、請求項39のテレビジョン会議データ管理システム。

【請求項41】 さらに、前記テレビジョン会議データを管理するテレビジョン会議データ管理プログラムが用いられる、請求項39又は請求項40のテレビジョン会議データ管理システム。

【請求項42】 さらに、暗号化されていない第2利用者情報が用いられる、請求項39、請求項340は請求項41のテレビジョン会議データ管理システム。

【請求項43】 前記暗号化されていない第2利用者情報が第2利用者情報ラベルとして前記暗号化テレビジョン会議データに付加されており、前記テレビジョン会議データが保存される場合、変更されたテレビジョン会議データが保存される場合、あるいは第2利用者にテレビジョン会議データが転送される場合には前記テレビジョン会議データとともに保存あるいは転送される、請求項

39、請求項40、請求項41又は請求項42のテレビジョン会議データ管理システム。

【請求項44】 前記第1利用者情報ラベルにデジタル署名がされている、請求項43のテレビジョン会議データ管理システム。

【請求項45】 第1利用者から第2利用者に暗号化されて供給されるテレビジョン会議データを利用するためのテレビジョン会議データ管理システムであって：該テレビジョン会議データ管理システムでは暗号鍵、利用者情報及びテレビジョン会議データ管理プログラムが利用され；前記第2利用者は前記第1利用者に第2利用者情報を提示し；前記第1利用者は前記第2利用者に第1暗号鍵で暗号化された前記テレビジョン会議データを供給し；前記第2利用者は前記テレビジョン会議データ管理プログラムを利用して前記第1暗号鍵に基づく第2暗号鍵を生成し；前記第2利用者が前記暗号化テレビジョン会議データを利用する場合には前記第1暗号鍵を用いて前記暗号化テレビジョン会議データが復号され；前記第2利用者が前記復号化テレビジョン会議データを保存、複製あるいは転送する場合には、前記復号化テレビジョン会議データが前記第2暗号鍵を用いて再暗号化される、テレビジョン会議データ管理システム。

【請求項46】 前記暗号鍵が秘密鍵である、請求項45のテレビジョン会議データ管理システム。

【請求項47】 前記暗号鍵が公開鍵及び専用鍵である、請求項45のテレビジョン会議データ管理システム。

【請求項48】 ユーザ端末装置のユーザ端末装置本体のシステムバスに接続して用いられ、

マイクログロッサ、マイクログロッサバスに接続された読み出し専用メモリ、書き込み・読み出しメモリ及び書換可能読み出し専用メモリから構成され、前記読み出し専用メモリには、データベース組織利用ソフトウェア及びユーザデータ等の固定した情報が格納され、

読み出し専用メモリには鍵管理センタあるいは著作権管理センタから供給される第1暗号鍵、第2暗号鍵及び著作権管理プログラムが格納される、データ著作権管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はデジタルデータの利用、保存、複製、加工、転送において著作権を管理するシステムに係るものであり、特にマルチメディアシステムに対して用いることを考慮したものである。

【0002】

【従来の技術】 情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつ

ある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム2値データであり、自然画及び動画のような情報量が格段に多いデータを取扱うことができなかった。

【0003】ところで、各種電気信号のデジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた2値データ以外の画像信号もデジタル処理技術の開発が進められている。この画像信号のデジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をデジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【0004】画像データは、文字データ及び音声データと比較して圧倒的に情報量が多いため、そのままでは保存、転送あるいはコンピュータにおける各種の処理が困難である。そのため、これらの画像データを圧縮／伸張することが考えられ、いくつかの画像データ圧縮／伸張用の規格が作成されてきた。その中で、共通の規格としてこれまでに静止画像用のJ P E G (Joint Photographic image coding Experts Group) 規格、テレビジョン会議用のH. 2 6 1規格、画像蓄積用のM P E G 1 (Moving Picture image coding Experts Group 1) 規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するM P E G 2規格が作成された。これらの技術により、デジタル映像データのリアルタイム処理が可能となってきた。

【0005】従来広く普及しているアナログデータは保存、複写、加工、転送をする毎に品質が劣化するため、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルデータは保存、複写、加工、転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルデータの著作権処理には的確な方法がなく、著作権法あるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0006】データベースの利用法は単にその内容を参照するだけでなく、通常は得たデータを保存、複写、加工することによって有効活用し、加工したデータを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオンラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログデータで

ある音声データ及び画像データがデジタル化されてデータベースとされる。

【0007】このような状況において、データベース化されたデータの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写、加工、転送等の2次利用について完成された著作権管理手段はない。本発明者らは特願平6-46419号及び特開平6-141004号で公衆電話回線を通じて鍵管理センタから利用許可鍵を入手することによって著作権管理を行うシステムを、特開平6-132916号でそのための装置を提案した。

【0008】また、特願平6-64889号において、これらの上記先願発明をさらに発展させることによって、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示（音声化を含む）、保存等の1次利用及び複写、加工、転送等の2次利用における著作権管理方法を提案した。

【0009】この先願のデータベース著作権管理システムは、著作権の管理を行うために、申し込まれた利用形態に対応した利用許可鍵の他に、著作権を管理するためのプログラム、著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を用いる。

【0010】著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0011】著作権管理プログラム、著作権情報及び著作権管理メッセージは、各々利用許可鍵とともに全体が供給される場合、データとともに全体が供給される場合及び一部が利用許可鍵とともに供給され、一部がデータとともに供給される場合がある。データ、利用許可鍵、著作権管理メッセージ、著作権情報及び著作権管理プログラムには、暗号化された状態で送信されるが利用時には暗号が解かれる場合、暗号化された状態で送信され表示の際のみに暗号が解かれその他の場合は暗号化された状態である場合、全く暗号化されない場合、の三つの場合がある。

【0012】

【発明の概要】本願においては先願である上記特願平6-64889号において提案されたデータ著作権管理方法を、具体的にしたデータ著作権管理システムを提供する。本発明においては、データ著作権管理システムを原データを保管するデータベース、暗号鍵を管理する鍵管理センタ、データ著作権を管理する著作権管理センタ及びこれらを相互に接続する通信ネットワークから構成し、データベースからユーザに供給されるデータは暗号化して配布され、ユーザは鍵管理センタあるいは著作権管理センタから入手した暗号鍵を用いて暗号化データを復号化して利用する。

【0013】ユーザへのデータ供給は暗号化データを放送等により一方向的に供給する方法と、暗号化データをユーザの要求に応じて双方向的に供給する方法がある。

【0014】データの暗号化に用いられる暗号鍵システムには秘密鍵システム、公開鍵システムあるいは秘密鍵と公開鍵を組み合わせたシステムが採用され、さらにデータ著作権を管理する著作権管理プログラムが採用される。

【0015】ユーザがデータを保存、複写あるいは転送する場合には、鍵管理センタあるいは著作権管理センタから供給される場合と、著作権管理プログラムによって生成される場合がある。

【0016】また、本発明は単一のデータだけではなく単一のデータベースから供給された複数のデータあるいは複数のデータベースから供給された複数のデータを利用する場合のデータ著作権管理システムにも適用可能である。また、あわせてデータ著作権管理を行うためにユーザ側で使用する装置についても提案する。

【0017】

【実施例】以下、本発明について説明するが初めに暗号技術について一般的な説明をしておく。暗号技術には、秘密鍵暗号方式 (secret-key cryptosystem) と、公開鍵暗号方式 (public-key cryptosystem) がある。秘密鍵暗号方式は、暗号化と復号化に同じ暗号鍵を使用する暗号方式であり、暗号化及び復号化に要する時間が短い反面、秘密鍵が発見され暗号が解読 (Cryptanalyze) されてしまうことがある。一方、公開鍵暗号方式は暗号化用の鍵が公開鍵 (public-key) として公開されており、復号化用の鍵が公開されていない暗号鍵方式であり、暗号化用の鍵は公開鍵と呼ばれ、復号化用の鍵は専用鍵 (private-key) と呼ばれる。この暗号方式を使用するには、情報を発信する側は暗号を受信する側の公開鍵で暗号化 (encryption) し、情報を受信する側は公開されていない専用鍵で復号化 (decryption) する暗号方式であり、暗号化及び復号化に要する時間が長い反面、専用鍵を発見することが殆ど不可能であり暗号の解読が非常に困難である。

【0018】暗号技術においては平文 (plaintext) M を暗号鍵 (cipher key) K を用いて暗号化し暗号文 (ciphertext) C を得る場合を

$$C = E(K, M)$$

と表現し、暗号文 C を暗号鍵 K を用いて復号し平文 M を得る場合を

$$M = D(K, C)$$

と表現する。本発明において使用される暗号方式には、暗号化と復号化に同じ秘密鍵 K_s が使用される秘密鍵方式 (secret-key system) と、平文の暗号化に公開鍵 (public key) K_b が使用され、暗号文の復号化に専用鍵 (private-key) K_v が使用される公開鍵方式 (public-key system) が採用される。

【0019】【実施例1】図1に示されたのは、本願発明に係るデータベース著作権管理システムの第1の実施例であり、この実施例1においては暗号鍵方式として秘密鍵方式が採用される。この図に示す実施例において、1はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、デジタル音声データ、デジタル映像データが暗号化された状態で格納されたデータベースであり、2は通信・放送衛星等の人工衛星、3はCD-ROMあるいはフレキシブルディスク等のデータ記録装置、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワーク、4は1次ユーザ端末装置である。また、9は秘密鍵を管理する鍵管理センタ、10はデータベース著作権を管理する著作権管理センタである。

【0020】5、6及び7は各々2次ユーザ端末装置、3次ユーザ端末装置及び n 次ユーザ端末装置であり、11、12及び13は各々フレキシブルディスクあるいはCD-ROM等の記憶媒体である2次ディスク、3次ディスク及び n 次ディスクである。なお、この n は任意の整数であり n が4よりも大きい場合には3次ユーザ端末装置6と n 次ユーザ端末装置7の間及び3次ディスク12と n 次ディスク13の間には対応するユーザ端末装置及びディスクが配置されている。

【0021】これらのうちデータベース1、鍵管理センタ9、著作権管理センタ10、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6及び n 次ユーザ端末装置7は通信ネットワーク8に接続されている。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースからの利用形態に対応した許可情報とともに秘密鍵が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録しておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に著作権管理プログラムを動作させるためのプログラムが含まれている。

【0022】データベース1あるいはデータ記録装置3に格納されているテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、デジタル音声データ、デジタル映像データである原データ M_0 が通信ネットワーク8、人工衛星2あるいは記憶媒体3を経由して1次ユーザ端末装置4に一方向的に供給されるが、このときには第1秘密鍵 K_{s1} を用いて暗号化される。

$$C_{m0k_{s1}} = E(K_{s1}, M_0)$$

なお、広告付等の無料で提供されるデータの場合でも著

著作権保護のためには、暗号化を必要とする。

【0023】前に述べた先願である特願平6-64889号には、データの利用形態には、最も基本的な表示の他に保存、加工、コピー、転送があり、利用許可鍵はこれらの利用形態のうちの1つあるいは複数に対応するものが用意され、その管理は著作権管理プログラムによって実行されることが示されている。また、データの表示及び加工のための表示以外の利用形態すなわちデータが保存、コピー、転送される場合には著作権管理プログラムによりデータが再暗号化されることが述べられている。いいかえれば、著作権が主張されたデータは暗号化された状態で流通し、平文化されるのは著作権処理機能を有するユーザ端末装置において、表示あるいは加工のための表示が行われるときのみである。

【0024】この実施例では、これら先願に記載された事項を利用する。供給された暗号化データCm0ks1の1次利用を希望する1次ユーザは鍵管理センタ9に対して1次ユーザ端末装置4を利用し通信ネットワーク8を経由して原データ名あるいは原データ番号等を指定することにより暗号化原データCm0ks1の1次利用申込を行うが、このときに1次ユーザに関する情報Iu1を鍵管理センタ9に提示する。1次ユーザ端末装置4を利用しての1次利用申込を受けた鍵管理センタ9は、著作権管理プログラムPとともに1次ユーザがデータベース1から入手した暗号化原データCm0ks1を復号化するための第1秘密鍵Ks1及び復号された原データM0あるいは原データを加工して得られた加工データM1を再暗号化するための第2秘密鍵Ks2を通信ネットワーク8を経由し1次ユーザ端末装置4に転送する。

【0025】復号鍵である第1秘密鍵Ks1、暗号化/復号化鍵である第2秘密鍵Ks2を受け取った1次ユーザ端末装置4において、初めに著作権管理プログラムPを利用して第1秘密鍵Ks1を用いて暗号化原データCm0ks1を復号化し

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。

【0026】原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4の内部、すなわちメモリあるいは内蔵のハードディスクドライブに保存されている状態ではそのデータを利用することができるのは1次ユーザのみであるが、データMがフレキシブルディスク等の外部記憶媒体11にコピーされた場合、あるいは通信ネットワーク8を経て2次ユーザ端末装置5に転送された場合には、2次利用による著作権の問題が生じる。

【0027】また、1次ユーザが入手した原データM0をそのまま複写して2次ユーザに供給した場合にはその原データM0に何等の改変も加えられていないため、そのデータM0に1次ユーザの著作権は発生しない。しか

し、1次ユーザが入手したデータM0を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータM1を作成した場合にはそのデータM1に1次ユーザの著作権(2次的著作権 secondarily exploitation right)が発生する。同様に、2次ユーザが1次ユーザから入手した原データM0あるいは加工データM1を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータM2を作成した場合には、同様に2次ユーザの著作権が発生する。

【0028】この著作権の問題に対処するため、この実施例においてはデータMの保存、コピー、転送が行われるときには著作権管理プログラムPにより第2秘密鍵Ks2を用いてデータMが暗号化され、以後1次ユーザ端末装置4においては第2秘密鍵Ks2を用いてデータMの復号化及び暗号化が行われる。

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2)$$

なお、1次ユーザがデータの表示及び加工を行い加工データを得ることは原則として自由にできるが、その場合は著作権管理プログラムによってその回数に制限を設けることができる。

【0029】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータが転送されたときには1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は著作権管理プログラムPによって廃棄される。したがって、1次ユーザが再度データMを利用する場合には鍵管理センタ9に利用申込を行い、第2秘密鍵Ks2の再交付を受ける必要がある。この第2秘密鍵Ks2の再交付を受けたことは、データMが外部記憶媒体11へコピーあるいは通信ネットワーク8を経由しての2次ユーザ端末装置5へ転送されることによる2次利用が行われたことを意味するから、このことが鍵管理センタ9から著作権管理センタ10に登録され、以後の2次利用が可能になる。

【0030】1次ユーザ端末装置4からの2次ユーザ端末装置5へのデータMの移動は外部記憶媒体11によってあるいは通信ネットワーク8により行われ、外部記憶媒体11へのコピーあるいは通信ネットワーク8を経由して移動が行われるときには、第2秘密鍵Ks2を用いてデータMが暗号化される。

【0031】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータMが転送されたときに1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は廃棄されるが、このときに1次ユーザ端末装置4内に保存されている暗号化データCmks2に、暗号化されていない1次ユーザ情報Iu1が付加され、暗号化データCmks2を2次ユーザに転送する際に1次ユーザ情報Iu1も転送される。

【0032】1次ユーザからコピーあるいは転送された

暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク8を経由して著作権管理センタ10に対して原データ名あるいは原データ番号を指定するとともに2次ユーザ情報Iu2を提示して2次利用申込を行うが、そのときに1次ユーザとの関係を明確にするために暗号化データCmks2に付加されている暗号化されていない1次ユーザ情報Iu1も提示する。著作権管理センタ10は、提示された1次ユーザ情報Iu1に基づきその1次ユーザがそのデータを2次利用するために第2秘密鍵Ks2の再交付を受けていることを確認し、復号化鍵である第2秘密鍵Ks2、暗号化/復号化鍵である第3秘密鍵Ks3を通信ネットワーク8を経由して2次ユーザ端末装置5に転送する。第2秘密鍵Ks2、第3秘密鍵Ks3を受け取った2次ユーザ端末装置5において、著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化データCmks2が復号化され $M = D(Ks2, Cmks2)$ 表示あるいは加工の2次利用が行われる。

【0033】この実施例においては、1次利用申込は鍵管理センタ9が処理し、2次利用申込は著作権管理センタ10が処理する。また、1次ユーザが供給されるデータMは第1秘密鍵Ks1を用いて暗号化されているが、2次ユーザが供給されるデータMは第2秘密鍵Ks2を用いて暗号化されている。一方、1次ユーザに対して鍵管理センタ9からは暗号鍵として第1秘密鍵Ks1及び第2秘密鍵Ks2が転送される。そのため、2次ユーザが1次ユーザであると偽って鍵管理センタ9に対して1次利用申込を行った場合には復号化鍵として第1秘密鍵Ks1が、暗号化/復号化鍵として第2秘密鍵Ks2が転送される。しかし、復号化鍵として転送された第1秘密鍵Ks1を用いて暗号化データCmks2を復号することはできない。したがって、データの利用について虚偽の申込を行うことは不可能であり、その結果データの原著作権だけでなく、データについての1次ユーザの著作権も保護される。

【0034】2次ユーザ端末装置5においてデータMの表示及び加工のための表示以外の利用形態である保存、コピー、転送が行われるときには著作権管理プログラムPによって第3秘密鍵Ks3を用いてデータMの暗号化が行われ、以後第3秘密鍵Ks3を用いてデータの復号及び暗号化が行われる。

$$Cmks3 = E(Ks3, M)$$

$$M = D(Ks3, Cmks3)$$

なお、2次ユーザが表示及び加工を行い加工データM2を得ることも原則として自由にできるが、その場合は著作権管理プログラムPによってその回数に制限を設けることができる。

【0035】外部記憶媒体12にデータMがコピーされたとき及び通信ネットワーク8を経てデータが転送されたときには2次ユーザ端末装置5内の第2秘密鍵Ks2及

び第3秘密鍵Ks3は著作権管理プログラムPによって廃棄される。したがって、2次ユーザが再度データMを利用するには著作権管理センタ10に利用申込を行い、第3秘密鍵Ks3の再交付を受ける必要がある。この第3秘密鍵Ks3の再交付を受けたことは、データMが外部記憶媒体12へコピーあるいは通信ネットワーク8を経由しての3次ユーザ端末装置6へ転送されることによる2次利用が行われたことを意味するから、このことが著作権管理センタ10に登録され、以後の利用が可能になる。

【0036】2次ユーザ端末装置5からの3次ユーザ端末装置6へのデータMの移動は外部記憶媒体12によってあるいは通信ネットワーク8により行われ、外部記憶媒体12へのコピーあるいは通信ネットワーク8を経由して移動が行われるときには、第3秘密鍵Ks3を用いてデータMが暗号化される。

【0037】外部記憶媒体12にデータMがコピーされたとき及び通信ネットワーク8を経てデータMが3次ユーザ端末装置6に転送されたときに2次ユーザ端末装置5内の第2秘密鍵Ks2及び第3秘密鍵Ks3は廃棄されるが、このときに2次ユーザ端末装置5内に保存されている暗号化データCmks3に、暗号化されていない2次ユーザ情報Iu2が付加される、暗号化データCmks3を3次ユーザに転送する際に2次ユーザ情報Iu2も転送される。この場合、各ユーザ情報のデータへの付加は、全てのユーザ情報がコピーあるいは転送の度にデータに付加される場合と、その度に最新のものに書き換えられる履歴が著作権管理センタに保管される場合がある。

【0038】2次ユーザからコピーあるいは転送された暗号化データCmks3の3次利用を希望する3次ユーザは、3次ユーザ端末装置6を利用して通信ネットワーク8を経由して著作権管理センタ10に対して原データ名あるいは原データ番号を指定するとともに3次ユーザ情報Iu3を提示して3次利用申込を行うが、そのときに2次ユーザとの関係を明確にするために暗号化データCmks3に付加されている暗号化されていない2次ユーザ情報Iu2も提示する。著作権管理センタ10は、提示された2次ユーザ情報Iu2に基づきその2次ユーザがそのデータを3次利用するための準備手続き、すなわち第3秘密鍵Ks3の再交付を受けていることを確認し、復号化鍵である第3秘密鍵Ks3、暗号化/復号化鍵である第4秘密鍵Ks4を通信ネットワーク8を経由して3次ユーザ端末装置6に転送する。第3秘密鍵Ks3、第4秘密鍵Ks4を受け取った3次ユーザ端末装置6において、著作権管理プログラムPにより第3秘密鍵Ks3を用いて暗号化データCmks3が復号化され $M = D(Ks3, Cmks3)$ 表示あるいは加工の3次利用が行われる。

【0039】この実施例においては、1次ユーザが供給されるデータMは第1秘密鍵Ks1を用いて暗号化され、

2次ユーザが供給されるデータMは第2秘密鍵Ks2を用いて暗号化されているが、3次ユーザが供給されるデータMは第3秘密鍵Ks3を用いて暗号化されている。そのため、3次ユーザが1次ユーザであると偽って鍵管理センタ9に対して1次利用申込を行った場合には復号化鍵として第1秘密鍵Ks1が、暗号化/復号化鍵として第2秘密鍵Ks2が転送される。しかし、復号化鍵として転送された第1秘密鍵Ks1を用いて暗号化データCmks3を復号化することはできない。また、3次ユーザが2次ユーザであると偽って著作権管理センタ9に対して2次利用申込を行った場合には復号化鍵として第2秘密鍵Ks2が、暗号化/復号化鍵として第3秘密鍵Ks3が転送される。しかし、復号化鍵として転送された第2秘密鍵Ks2を用いて暗号化Cmks3を復号することはできない。したがって、データの利用について虚偽の申込を行うことは不可能であり、その結果データの著作権だけでなく、データについての1次ユーザの著作権及び2次ユーザの著作権も保護される。以下、同様の手続きが4次以降の利用にも適用される。

【0040】以上説明した実施例におけるデータベース1、鍵管理センタ9、著作権管理センタ10は別個に設置されているが、これらは必ずしも別個のものである必要はなく、これらの全てあるいは適当な2つを一体に設置することも可能である。また、1次ユーザからの2次暗号鍵再交付申込は実施例のように鍵管理センタ9に対して行うのではなく著作権管理センタ10に対して行うようにしてもよい。

【0041】[実施例2]次に、実施例2について説明するが、この実施例の大部分の構成は実施例1の構成と同様であるが、著作権管理プログラム、場合によってはさらに第1秘密鍵と第2秘密鍵が、暗号化されて供給される。この実施例でも第1実施例と同様に原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。なお、実施例2で用いるシステム構成は図1に示された実施例1のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【0042】この実施例において、データベース1に格納されている原データM0が人工衛星2、記憶媒体3あるいは通信ネットワーク8を経由して1次ユーザ端末装置4に一方向的に供給されるが、そのときには第1秘密鍵Ks1を用いて暗号化される。

$$Cm0ks1 = E(Ks1, M0)$$

【0043】供給された暗号化データCm0ks1の1次利用を希望する1次ユーザは鍵管理センタ9に対して1次ユーザ端末装置4を利用し通信ネットワーク8を経由して原データ名あるいは原データ番号等を指定することにより暗号化原データCm0ks1の1次利用申込を行うが、このときに1次ユーザ情報Iu1を鍵管理センタ9に提示する。

【0044】暗号化原データCm0ks1の1次利用申込を受けた鍵管理センタ9は、1次ユーザ情報Iu1を利用して1次ユーザ専用の秘密鍵Ksulを生成し著作権管理センタ10に転送する。

【0045】1次ユーザ専用の秘密鍵Ksulを受け取った著作権管理センタ10は、この1次ユーザ専用秘密鍵Ksulを用いて著作権管理プログラムPを暗号化し、

$Cpksul = E(Ksul, P)$
暗号化著作権管理プログラムCpksulを鍵管理センタ9に転送する。このようにして生成された暗号化著作権管理プログラムCpksulは1次ユーザに固有のものである。また、鍵管理センタ9は著作権管理センタ10から受け取った暗号化著作権管理プログラムCpksulとともに復号化鍵である第1秘密鍵Ks1及び復号化/暗号化鍵である第2秘密鍵Ks2を通信ネットワーク8を経由し1次ユーザ端末装置4に転送する。

【0046】暗号化著作権管理プログラムCpksul、第1秘密鍵Ks1、第2秘密鍵Ks2を受け取った1次ユーザ端末装置4において、初めに予め配布されているデータベース組織用ソフトウェアSが1次ユーザ情報Iu1に基づいて1次ユーザ専用秘密鍵Ksulを生成し、

$Ksul = S(Iu1)$
生成された1次ユーザ専用秘密鍵Ksulを用いて暗号化著作権管理プログラムCpsulを復号化し、

$P = D(Ksul, Cpsul)$
復号化された著作権管理プログラムPを利用して第1秘密鍵Ks1を用いて暗号化原データCm0ks1を復号化し

$M0 = D(Ks1, Cm0ks1)$
復号化された原データM0をそのままあるいは加工データM1として利用する。

【0047】原データM0あるいは加工データM1であるデータMの保存、コピー、転送が行われるときには著作権管理プログラムPにより第2秘密鍵Ks2を用いてデータMが暗号化され、以後1次ユーザ端末装置4においては第2秘密鍵Ks2を用いてデータMの復号化及び暗号化が行われる。

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2)$$

【0048】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータが転送されたときには1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は著作権管理プログラムPによって廃棄される。したがって、1次ユーザが再度データMを利用する場合には鍵管理センタ9に利用申込を行い、第2秘密鍵Ks2の再交付を受ける必要がある。この第2秘密鍵Ks2の再交付を受けたことは、データMが外部記憶媒体11へコピーあるいは通信ネットワーク8を経由しての2次ユーザ端末装置5へ転送されることによる2次利用が行われたことを意味するから、このことが鍵管理センタ9から著作権管理センタ10に登録され、以後の2

次利用が可能になる。

【0049】1次ユーザ端末装置4からの2次ユーザ端末装置5へのデータMの移動は外部記憶媒体11によってあるいは通信ネットワーク8により行われる。データMの外部記憶媒体11へのコピーあるいは通信ネットワーク8を経由して転送が行われるときには、第2秘密鍵Ks2を用いてデータMが暗号化される。

【0050】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータMが転送されたときに1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は廃棄されるが、このときに1次ユーザ端末装置4内に保存されている暗号化データCmks2に、1次ユーザについての暗号化されていない情報Iu1が付加される。そのため、暗号化データCmks2を2次ユーザに転送する際に1次ユーザ情報Iu1も転送される。

【0051】1次ユーザからコピーあるいは転送された暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク8を経由して著作権管理センタ10に対して原データ名あるいは原データ番号を指定するとともに2次ユーザ情報Iu2を提示して2次利用申込を行うが、そのときに1次ユーザとの関係を明確にするために暗号化データCmks2に付加されている暗号化されていない1次ユーザ情報Iu1も提示する。著作権管理センタ10は、提示された1次ユーザ情報Iu1に基づきその1次ユーザがそのデータを2次利用するために第2秘密鍵Ks2の再交付を受けていることを確認し、提示された2次ユーザ情報Iu2に基づいて2次ユーザ専用の秘密鍵Ksu2を生成する。

【0052】著作権管理センタ10はこの2次ユーザ専用秘密鍵Ksu2を用いて著作権管理プログラムPを暗号化し、

$$Cpksu2 = E(Ksu2, P)$$

暗号化著作権管理プログラムCpksu2、復号化鍵である第2秘密鍵Ks2、暗号化／復号化鍵である第3秘密鍵Ks3を通信ネットワーク8を経由して2次ユーザ端末装置5に転送する。なお、この暗号化著作権管理プログラムCpksu2に1次ユーザに関する情報Iu1を付加しておいてもよい。

【0053】第2秘密鍵Ks2、第3秘密鍵Ks3を受け取った2次ユーザ端末装置5において、データベース組織利用ソフトウェアが2次ユーザ情報Iu2に基づいて2次ユーザ専用秘密鍵Ksu2を生成し、

$$Ksu2 = S(Iu2)$$

生成された2次ユーザ専用秘密鍵Ksu2を用いて暗号化著作権管理プログラムCpsu2を復号化し、

$$P = D(Ksu2, Cpksu2)$$

復号化された著作権管理プログラムPを利用して第2秘密鍵Ks2を用いて暗号化原データCmks2を復号化し

$$M = D(Ks2, Cmks2)$$

復号化されたデータMをそのままあるいは加工して利用

する。

【0054】このように、利用申込を行ったユーザのユーザ情報に基づいてユーザ専用暗号鍵を生成し、生成されたユーザ専用暗号鍵を用いて著作権管理プログラムを暗号化することにより、データ著作権管理システムの安全性が高くなる。また、このときにユーザに供給される各秘密鍵もユーザ専用暗号鍵を用いて暗号化すれば、データ著作権管理システムの安全性がより高くすることができる。

【0055】【実施例3】さらに、図1に示されたシステムにおいて、外部記憶媒体11にデータMがコピーされた場合、あるいは通信ネットワーク8を経てデータMが転送された場合に生じる著作権の問題に対応するためのさらに別の方法として、1次ユーザ端末4の利用者が行う1次利用申込を表示許可、保存許可及び加工許可だけに限定しそれ以外の利用申込すなわちコピー許可及び転送許可を受けることはできず、コピー許可及び転送許可の申込は別に行うようにし、外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータが2次ユーザ端末装置5に転送されたときに、1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は廃棄されるようにすることもできる。このようにすれば、データMのコピーあるいは転送をより確実に著作権管理センタ10で把握することができる。

【0056】【実施例4】図2に示されたのは、本願発明に係るデータ著作権管理システムの実施例4の構成である。図1に示されたシステムでは、暗号化データが衛星2、記録媒体3あるいは通信ネットワーク8を経由して一方向的に供給されるが、実施例2では1次ユーザ4からの要求に応じて暗号化データが双方向的に供給される。また、この実施例においては、暗号鍵方式として公開鍵方式が採用される。なお、実施例2がデータ供給手段としてデータベース以外に広告付き等の無料の暗号化する必要の無い衛星放送、地上波放送、CATV放送あるいは記録媒体を用いる場合にも適用可能なことは勿論のことである。

【0057】図1に示されたシステムと同様にこの図に示されたシステムにおいて、1はデータベース、4は1次ユーザ端末装置、5は2次ユーザ端末装置、6は3次ユーザ端末装置、7はn次ユーザ端末装置である。また、14は2次著作権管理センタ、15は3次著作権管理センタ、16はn次著作権管理センタ、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワークである。

【0058】これらのうち、データベース1、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6、n次ユーザ端末装置7、2次著作権管理センタ14、3次著作権管理センタ15、n次著作権管理センタ16は通信ネットワーク8に接続されており相互に接

続可能である。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースからの利用形態に対応した許可情報とともに暗号鍵が転送される経路であり、2点鎖線で示された経路はデータベースあるいは各著作権管理センタデータベースから次位の著作権管理センタデータベースへ著作権情報が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録しておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信ソフトウェアの他に暗号化された著作権管理プログラムを復号化するためのプログラムが含まれている。

【0059】データベース1を利用するに当たり、1次ユーザは1次ユーザ認証データAu1、第1公開鍵Kb1及び第1公開鍵Kb1に対応する第1専用鍵Kv1、第2公開鍵Kb2及び第2公開鍵Kb2に対応する第2専用鍵Kv2を用意し、1次ユーザ端末装置4を利用し通信ネットワーク8を経由してデータベース1にアクセスする。

【0060】1次ユーザから1次ユーザ認証データAu1、第1公開鍵Kb1、第2公開鍵Kb2の転送を受けたデータベース1は、1次ユーザ認証データAu1を確認し、確認された1次ユーザ認証データAu1を1次ユーザ情報Iu1として2次著作権管理センタ14に転送する。

【0061】一方、データベース1は2個の秘密鍵すなわち第1の秘密鍵Ks1と第2の秘密鍵Ks2を用意する。この2個の秘密鍵の用意は図1に示された実施例1の鍵センタ9を利用して行ってもよい。用意された第1の秘密鍵Ks1及び第2の秘密鍵Ks2中、第2の秘密鍵Ks2も予め著作権管理センタ14に転送される。

【0062】これらの転送が行われた結果著作権管理センタ14には1次ユーザ情報Iu1、原著作権情報Ic及び第2秘密鍵Ks2が格納される。なお、これらの中で原著作権情報Icは著作権使用料分配に用いられる。

【0063】データの利用を希望する1次ユーザは、1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0064】データメニューが転送されると1次ユーザはデータメニュー検索を行いデータMを選択する。このとき、選択されたデータMの原著作権情報Icが著作権管理センタ14に転送される。

【0065】1次ユーザの要求に応じてデータベース1から原データM0が読み出される。読み出された原データM0は第1秘密鍵Ks1で暗号化される。

$$Cm0ks1 = E(Ks1, M0)$$

この暗号化データCm0ks1には暗号化されていない原著作権者情報Icが付けられている。また、第1の秘密鍵

Ks1を第1の公開鍵Kb1で、第2の秘密鍵Ks2を同じく第2の公開鍵Kb2で暗号化する。

$$Cks1kb1 = E(Kb1, Ks1)$$

$$Cks2kb2 = E(Kb2, Ks2)$$

併せて著作権管理プログラムPも第2の秘密鍵Ks2で暗号化されるが、

$$Cpks2 = E(Ks2, P)$$

著作権管理プログラムPの暗号化は第2の秘密鍵Ks2で暗号化されなければならないものではなく、他の適当な暗号鍵を用いて暗号化することができる。暗号化原データCm0ks1、暗号化著作権管理プログラムCpks2及び2個の暗号化秘密鍵Cks1kb1、Cks2kb2が通信ネットワーク8を経由して1次ユーザ端末装置4に転送される。このときに必要ならば課金が行われる。なお、暗号化著作権管理プログラムCpks2はデータベース1から供給されるのではなく、ユーザ端末装置4内の例えばROMに内蔵しておくことも可能である。

【0066】データベース1から暗号化原データCm0ks1、2個の暗号化秘密鍵Cks1kb1、Cks2kb2及び暗号化著作権管理プログラムCpks2を受け取った1次ユーザは、データベース組織利用ソフトウェアを利用して第1公開鍵Kb1に対応する第1専用鍵Kv1を用いて暗号化第1秘密鍵Cks1kb1を復号化し、

$$Ks1 = D(Kv1, Cks1kb1)$$

第2公開鍵Kb2に対応する第2専用鍵Kv2を用いて暗号化第2秘密鍵Cks2kb2を復号化する。

$$Ks2 = D(Kv2, Cks2kb2)$$

さらに、復号化された第2秘密鍵Ks2を用いて暗号化著作権管理プログラムCpks2を復号化する。

$$P = D(Ks2, Cpks2)$$

【0067】最後に、復号化された著作権管理プログラムPを利用して復号化された第1秘密鍵Ks1を用いて暗号化データCm0ks1を復号化し、

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。前に説明したように、第1専用鍵Kv1及び第2専用鍵Kv2は1次ユーザが用意他には公開していない暗号鍵であるから、第3者がデータMを入手したとしても暗号化データMを復号化して利用することは不可能である。

【0068】以後原データM0あるいは加工データM1であるデータMの保存、コピーあるいは転送を行う場合には第2秘密鍵Ks2を用いて暗号化及び復号が行われる。

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2)$$

復号された第2の秘密鍵Ks2は以後データの保存、コピーあるいは転送を行う場合にデータの暗号化/復号化を行う際の暗号鍵として用いられる。1次ユーザ端末装置4には、これらの第1専用鍵Kv1及び第2専用鍵Kv2、第1の秘密鍵Ks1及び第2秘密鍵Ks2、データM、著作権

権管理プログラムPとともに原著作権情報Ic及び1次ユーザがデータの加工を行った場合には1次ユーザ情報及び加工日時等である著作権情報Ic1も格納される。なお、この著作権情報Ic1は著作権情報ラベルとしてデータに付けるようにし、さらにデジタル署名付にしておけば安全である。暗号化データCmks2は暗号化されて流通し、復号鍵である第2秘密鍵Ks2を入手するためには、著作権情報ラベルが手がかりとなるから、暗号化データCmks2からこの著作権情報ラベルが取り外された場合には、第2秘密鍵Ks2を入手することができない。

【0069】暗号化データCmks2が1次ユーザ端末装置4内に保存された場合には第2の秘密鍵Ks2が装置内に保存されるが、暗号化データCmks2が1次ユーザ端末装置4内に保存されることなく記憶媒体11にコピーあるいは通信ネットワーク8を経由して2次ユーザ端末装置5への転送が行われた場合には、1次ユーザ端末装置4における以降の利用を不可能にするために第2の秘密鍵Ks2が廃棄される。なお、この場合コピー・転送回数に制限を設けて、制限回数内のコピー・転送では第2の秘密鍵Ks2が廃棄されないようにしてもよい。

【0070】データMを外部記憶媒体11にコピーあるいは通信ネットワーク8を経由して転送しようとする1次ユーザは、コピーあるいは転送を行うにあたって第2秘密鍵Ks2を用意し、データMを第2の秘密鍵Ks2を用いて暗号化する。

$$Cmks2 = E(Ks2, M)$$

この暗号化データCmks2には暗号化されていない原著作権情報Ic、1次ユーザの著作権情報Ic1が付加される。

【0071】2次ユーザは、データベース使用前に1次ユーザと同様に2次ユーザを認証するための認証データAu2、第3の公開鍵Kb3及び第3の公開鍵Kb3に対応する第3の専用鍵Kv3、第4の公開鍵Kb4及び第4の公開鍵Kb4に対応する第4の専用鍵Kv4を用意する。

【0072】コピーあるいは転送された暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク8を経由して2次著作権管理センタ14に対して原データ名あるいは原データ番号を指定して2次利用申込を行うが、そのときに、2次ユーザ認証データAu2、原著作権情報Ic及び1次ユーザ著作権情報Ic1に加えて第3の公開鍵Kb3と第4の公開鍵Kb4も転送する。

【0073】2次ユーザからの2次利用申込を受けた2次著作権管理センタ14は、2次ユーザの認証データAu2を確認し、確認された2次ユーザ認証データAu2は2次ユーザ情報として3次著作権管理センタ15に転送される。また、1次ユーザの2次著作権情報Ic1が転送された場合には2次的著作権情報Ic1を2次著作権管理センタ14に照会・確認し、確認された2次的著作権情報Ic1は3次著作権管理センタ15に転送される。

【0074】2次著作権管理センタ14は、第3の秘密鍵Ks3を用意する。この第3の秘密鍵Ks3は実施例1に示された鍵センタ9を利用して用意してもよい。用意された第3の秘密鍵Ks3は3次著作権管理センタ15に転送され格納される。

【0075】これらの転送が行われた結果、3次著作権管理センタ15には1次ユーザ著作権情報Ic1、1次ユーザ情報I1、原著作権情報Ic、2次ユーザ情報Iu2及び第3の秘密鍵Ks3が格納される。これらの中、1次ユーザ著作権情報Ic1及び1次ユーザ情報I1は、著作権使用料金分配に用いられる。

【0076】以下同様にして、n次著作権管理センタ16には(n-1)次ユーザの2次的著作権情報Icn-1、1次ユーザ情報I1、原著作権情報Ic、n次ユーザ情報In及び第nの秘密鍵Ksnが格納される。

【0077】2次著作権管理センタ14から1次ユーザ情報I1、原著作権情報Ic及び第2の秘密鍵Ks2が読み出される。この中、原著作権情報Icは著作権使用料配分のために使用される。読み出された第2の秘密鍵Ks2は2次ユーザの第3の公開鍵Kb3を用いて、第3の秘密鍵Ks3は同じく第4の公開鍵Kb4を用いて暗号化される。

$$Cks2kb3 = E(Kb3, Ks2)$$

$$Cks3kb4 = E(Kb4, Ks3)$$

また、著作権管理プログラムPは第3の秘密鍵Ks3を用いて、第3の秘密鍵Ks3は第4の公開鍵Kb4を用いて暗号化される。

$$Cpks3 = E(Ks3, P)$$

$$Cks3kb4 = E(Kb4, Ks3)$$

暗号化著作権管理プログラムCpks3及び暗号化第2秘密鍵Cks2kb3及び暗号化第3秘密鍵Cks3kb4が通信ネットワーク8を経由して2次ユーザ端末装置3に転送される。このときに必要ならば課金が行われる。

【0078】2次著作権管理センタ14から暗号化された2個の秘密鍵Cks2kb3及びCks3kb4及び暗号化された著作権管理プログラムCpks3を受け取った2次ユーザは、データベース利用ソフトウェアを利用して第3専用鍵Kv3を用いて暗号化第2秘密鍵Cks2kb3を復号し、第4の公開鍵Kb4に対応する第4の専用鍵Kv4を用いて暗号化第3秘密鍵Cks3kb4を復号する。

$$Ks2 = D(Kv3, Cks2kb3)$$

$$Ks3 = D(Kv4, Cks3kb4)$$

また、復号化された第3の秘密鍵Ks3を用いて暗号化著作権管理プログラムCpks3が復号される。

$$P = D(Ks3, Cpks3)$$

次に、復号化された著作権管理プログラムPを利用して復号された第2の秘密鍵Ks2を用いて暗号化データCmks2を復号化し利用する。

$$M = D(Ks2, Cmks2)$$

【0079】前に説明したように、第3専用鍵Kv3及び

第4専用鍵Kv4は2次ユーザが用意しただけで他には公開していない暗号鍵であるから、第3者が暗号化データCmks2を入手したとしても復号化して利用することは不可能である。

【0080】以上説明した実施例において、データベース1、2次著作権管理センタ14、3次著作権管理センタ15及びn次著作権管理センタ16は、利用申込の輻輳を避けるために別個に設けられている。しかし、利用申込の輻輳が問題とならないならば、これらの全部あるいは一部を合体させることもできる。

【0081】〔実施例5〕図3に示されたのは、実施例5のシステム構成であり、この実施例5において、原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。この実施例において、暗号鍵方式に秘密鍵方式が採用される。

【0082】この図において、1はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、ディジタル音声データ、ディジタル映像データが暗号化された状態で格納されたデータベースであり、2は通信・放送衛星等の人工衛星、3はCD-ROMあるいはフレキシブルディスク等のデータ記録媒体、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワーク、4は1次ユーザ端末装置である。また、17はデータの著作権を管理する著作権管理センタであり、5、6及び7は各々2次ユーザ端末装置、3次ユーザ端末装置及びn次ユーザ端末装置である。

【0083】これらのうちデータベース1、著作権管理センタ17、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6及びn次ユーザ端末装置7は通信ネットワーク8によって相互に接続可能とされている。

【0084】このシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要がある。また、この登録の際にデータベース利用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信プロトコル等の通常の通信ソフトウェアプログラムが含まれている。このデータベース組織を利用するためのソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置内に蔵されるマスクROM、EPROM、EEPROM等に格納することも可能である。

【0085】また、このシステムにおいてはユーザ側で秘密鍵を生成するため、ユーザ端末装置に秘密鍵生成アルゴリズムが格納されるが、この秘密鍵生成アルゴリズム自身は必ずしも秘密のものではないため、データベース組織に対して利用を登録するときにユーザに対して供給されるデータベース組織利用ソフトウェアに内蔵させ

てもよい。なお、原データが広告付等無料で供給される場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。

【0086】この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースから暗号鍵が転送される経路である。

10 【0087】データベース1あるいはデータ記録媒体3に格納されている原データM0は通信ネットワーク8を経由して有線経路で、人工衛星2等を経由して放送電波によりあるいは記録媒体3を経由して1次ユーザ端末装置4に供給されるがこのときに第1秘密鍵Ks1を用いて暗号化される。

$Cm0ks1 = E(Ks1, M0)$

20 【0088】実施例1～4の場合と同様に、暗号化されて供給される原データCm0ks1の著作権を保護するために、本発明者らによる先願である特願平6-64889号に示されているように、1次ユーザ端末装置4において、原データM0は、表示及び加工のための表示以外の利用形態である保存、コピー、転送が行われるときには第2秘密鍵Ks2を用いて暗号化され、

$Cm0ks2 = E(Ks2, M0)$

以後の利用においては第2秘密鍵Ks2によって原データの暗号化/復号化が行われる。

30 【0089】暗号化原データCm0ks1を入手した1次ユーザは1次ユーザ端末装置4を利用して、原データ名あるいは原データ番号等を指定して、暗号化原データCm0ks1の1次利用を著作権管理センタ17に申し込む。1次ユーザ端末装置4から暗号化原データCm0ks1の1次利用申込を受けた著作権管理センタ17は、第1秘密鍵Ks1とともに著作権管理プログラムPを1次ユーザ端末装置4に転送する。この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムにより秘密鍵の生成及びデータの復号化/暗号化が行われる。

40 【0090】第1秘密鍵Ks1と著作権管理プログラムPを受け取った1次ユーザ端末装置4は、暗号プログラムを利用して第1秘密鍵Ks1を用いて暗号化原データCm0ks1を復号し、

$M0 = D(Ks1, Cm0ks1)$

復号化された原データM0をそのままあるいは加工データM1として利用する。また、著作権管理プログラムPにより第1秘密鍵Ks1に基づいて第2秘密鍵Ks2が生成される。

$Ks2 = P(Ks1)$

50 【0091】原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、2次ユーザ端末装置5

に転送される場合には、著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$Cmks2 = E(Ks2, M)$

【0092】第2秘密鍵Ks2によって暗号化されたデータCmks2は、原データ名あるいは原データ番号とともに、記録媒体11に複写あるいは通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0093】暗号化されたデータCmks2を入手した2次ユーザは2次ユーザ端末装置5を利用して、原データ名あるいは原データ番号を指定することにより暗号化データCmks2の2次利用を著作権管理センタ17に申し込む。

【0094】暗号化データCmks2の2次利用申込を受けた著作権管理センタ17は、原データ名あるいは原データ番号から第1秘密鍵Ks1を探し出し、著作権管理プログラムPにより第1秘密鍵Ks1から第2秘密鍵Ks2を生成し、

$Ks2 = P(Ks1)$

生成された第2秘密鍵Ks2を著作権管理プログラムPとともに2次ユーザ端末装置5に供給する。

【0095】第2秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザ端末装置5は、第2秘密鍵Ks2で暗号化されたデータCmks2を第2秘密鍵Ks2で復号化して

$M = D(Ks2, Cmks2)$

表示あるいは加工の利用を行う。

【0096】復号されたデータMが2次ユーザ端末装置5内に保存される場合、記録媒体12に保存される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータMは著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

【0097】さらに、著作権管理プログラムPが、第2秘密鍵Ks2に基づいて第3秘密鍵Ks3を生成するようにし、

$Ks3 = P(Ks2)$

【0098】データMが2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータMは著作権管理プログラムPにより第3の秘密鍵Ks3を用いて暗号化されるようにしてもよい。

$Cmks3 = E(Ks3, M)$

【0099】〔実施例6〕次に、実施例6について説明するが、実施例5と同様に原データは単一のデータベースから暗号化されて一方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。この実施例において採用される暗号鍵方式は秘密鍵方式であり、第2秘密鍵は1次ユーザ情報と第1秘密鍵に基づいて生成される。なお、実施例6で用いるシステム構成

は図3に示された実施例5のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【0100】実施例6において、データベース1に格納されている原データM0は通信ネットワーク8を経由して有線経路で、人工衛星2等経由して放送電波によりあるいは記録媒体3を経由して第1秘密鍵Ks1を用いて暗号化されて

$Cm0ks1 = E(Ks1, M0)$

1次ユーザ端末装置4に供給される。

【0101】暗号化原データCm0ks1を入手した1次ユーザは1次ユーザ端末装置4を利用して、暗号化原データCm0ks1の1次利用を著作権管理センタ17に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに1次ユーザ情報Iu1を提示する。

【0102】1次ユーザから暗号化原データCm0ks1の1次利用申込を受けた著作権管理センタ17は、第1秘密鍵Ks1と著作権管理プログラムPを1次ユーザ端末装置4に供給する。

【0103】著作権管理プログラムPには、暗号アルゴリズムを有する暗号プログラムPが含まれており、この暗号プログラムPにより秘密鍵生成及び復号/暗号化が行われる。

【0104】第1秘密鍵Ks1と著作権管理プログラムを受け取った1次ユーザ端末装置4では、暗号プログラムPにより第1秘密鍵Ks1を用いて暗号化原データM0を復号して

$M0 = D(Ks1, Cm0ks1)$

復号化された原データM0をそのままあるいは加工データM1として利用する。また、供給された著作権管理プログラムPが、1次ユーザ情報Iu1あるいは1次ユーザ情報Iu1と第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成する。

$Ks2 = P(Iu1)$ 又は

$Ks2 = P(Iu1 + Ks1)$

生成された第2秘密鍵Ks2は1次ユーザ情報Iu1に基づいているため、正しい1次ユーザ情報Iu1を有していなければ生成することが不可能である。なお、1次ユーザ情報Iu1に代えて、1次ユーザ情報Iu1に基づいて生成された1次ユーザデータ、あるいは1次ユーザ端末装置4に付与されている装置番号を利用することもできる。

【0105】原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に供給される場合には、そのデータMは著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$Cmks2 = E(Ks2, M)$

【0106】第2秘密鍵Ks2で暗号化されたデータCmks2は、原データ名あるいは原データ番号及び1次ユーザ情報Iu1とともに、記録媒体11に複写されあるいは、

通信ネットワーク 8 を経由して 2 次ユーザ端末装置 5 に供給される。

【0107】暗号化されたデータ $Cmks2$ を入手した 2 次ユーザは 2 次ユーザ端末装置 5 を利用して、データ M の 2 次利用を著作権管理センタ 17 に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに 1 次ユーザ情報 $Iu1$ を提示する。

【0108】データ M の 2 次利用申込を受けた著作権管理センタ 17 は、原データ名あるいは原データ番号を手がかりとして第 1 秘密鍵 $Ks1$ を探し出し、1 次ユーザ情報 $Iu1$ 、第 1 秘密鍵 $Ks1$ あるいは 1 次ユーザ情報 $Iu1$ と第 1 秘密鍵 $Ks1$ に基づいて第 2 秘密鍵 $Ks2$ を生成し、生成された第 2 秘密鍵 $Ks2$ を著作権管理プログラム P とともに 2 次ユーザ端末装置 5 に提供する。

【0109】第 2 秘密鍵 $Ks2$ と著作権管理プログラム P を受け取った 2 次ユーザは 2 次ユーザ端末装置 5 を利用して、著作権管理プログラム P により第 2 秘密鍵 $Ks2$ を用いて暗号化データ $Cmks2$ を復号化して利用する。

$M = D(Ks2, Cmks2)$

データ M が 2 次ユーザ端末装置 5 内に保存される場合、記録媒体 11 に複写される場合、通信ネットワークを経由して 3 次ユーザ端末装置 6 に供給される場合には、そのデータは第 2 秘密鍵 $Ks2$ によって暗号化される。

【0110】なお、著作権管理プログラム P により第 2 秘密鍵 $Ks2$ に基づいて第 3 秘密鍵 $Ks3$ を生成するようにし、

$Ks3 = P(Ks2)$

データ M が 2 次ユーザ端末装置 5 内に保存される場合、記録媒体 11 に複写される場合、通信ネットワークを経由して 3 次ユーザ端末装置 6 に供給される場合には、そのデータは第 3 秘密鍵 $Ks3$ によって暗号化されるようにすることもできる。

【0111】また、2 次ユーザが著作権管理センタ 17 に 2 次利用申込を行うときに、2 次ユーザ情報 $Iu2$ を提示し、提示された 2 次ユーザ情報 $Iu2$ に基づいて第 3 秘密鍵 $Ks3$ が生成されるようにすることもできる。

【0112】この実施例 6 において、第 2 秘密鍵 $Ks2$ を生成する著作権管理プログラム P を全データベース組織において共通のものとしておけば、どのデータベース組織においても 1 次ユーザ情報 $Iu1$ 及び第 1 秘密鍵 $Ks1$ が変更されない限り同一の原データに対しては同一の第 2 秘密鍵 $Ks2$ が生成される。

【0113】【実施例 7】次に、実施例 7 について説明するが、実施例 5 及び実施例 6 と同様原データは単一のデータベースから暗号化されて 1 方向的に供給され、ユーザは供給された原データから必要なものを選択して利用する。また、この実施例において第 2 秘密鍵は著作権管理プログラム P の使用回数と第 1 秘密鍵に基づいて生成される。

は秘密鍵方式である。なお、実施例 7 で用いるシステム構成は図 3 に示された実施例 5 及び実施例 6 のシステム構成と異なる点はないため、システム構成についての説明は省略する。

【0115】データベース 1 に格納されている原データ $M0$ は通信ネットワーク 8 を経由して有線経路で、人工衛星 2 等を経由して放送電波によりあるいは記録媒体 3 を経由して第 1 秘密鍵 $Ks1$ を用いて暗号化されて $Cm0ks1 = E(Ks1, M0)$

1 次ユーザ端末装置 4 に供給される。

【0116】暗号化原データ $Cm0ks1$ を入手した 1 次ユーザは 1 次ユーザ端末装置 4 を利用して、原データ名あるいは原データ番号等を指定することにより原データ $M0$ の 1 次利用を著作権管理センタ 17 に申し込む。

【0117】原データ $M0$ の 1 次利用申込を受けた著作権管理センタ 17 は、第 1 秘密鍵 $Ks1$ 及び著作権管理プログラム P を 1 次ユーザ端末装置 4 に転送する。

【0118】この著作権管理プログラム P には暗号アルゴリズムを有する暗号プログラムが含まれており、暗号鍵の生成及びデータの復号化／暗号化が行われる。また、著作権管理プログラム P にはカウンタが付属しており、このカウンタがプログラム P の使用回数 N を計数する。

【0119】第 1 秘密鍵 $Ks1$ 及び著作権管理プログラム P を受け取った 1 次ユーザは、暗号化原データ $Cm0ks1$ を著作権管理プログラム P を利用して第 1 秘密鍵 $Ks1$ を用いて復号化して

$M0 = D(Ks1, Cm0ks1)$

復号化された原データ $M0$ をそのままあるいは加工データ $M1$ として利用する。

【0120】このシステムにおいては、データの著作権を管理するために原データ $M0$ あるいは加工データ $M1$ であるデータ M が 1 次ユーザ端末装置 4 内に保存される場合、記録媒体 11 に複写される場合、通信ネットワーク 8 を経由して 2 次ユーザ端末装置 5 に転送される場合に著作権管理プログラム P により第 2 秘密鍵 $Ks1$ を用いて暗号化されるが、このときに用いられる第 2 暗号鍵 $Ks2$ は著作権管理プログラム P の使用回数 N と第 1 秘密鍵 $Ks1$ に基づいて生成される。

$Ks2 = P(N + Ks1)$

【0121】このようにして生成される第 2 秘密鍵 $Ks2$ は著作権管理プログラム P の使用回数 N と第 1 秘密鍵 $Ks1$ に基づいているため、データ M は利用される度に最新の第 2 秘密鍵 $Ks2$ で暗号化される。

$Cmks2 = E(Ks2, M)$

【0122】最後の利用によって生成された第 2 秘密鍵 $Ks2$ によって暗号化されたデータ $Cmks2$ は、原データ名あるいは原データ番号、カウンタデータ $N1$ とともに、記録媒体 11 に複写あるいは、通信ネットワーク 8 を経

【0123】暗号化データCmks2を入手した2次ユーザは2次ユーザ端末装置5を用いて、原データ名あるいは原データ番号及びカウンタデータN1を提示して、暗号化データCmks2の2次利用を著作権管理センタ17に申し込む。

【0124】暗号化データCmks2の2次利用申込を受けた著作権管理センタ17は、提示された原データ名あるいは原データ番号から第1秘密鍵Ks1を探し出し、カウンタデータN1及び第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、著作権管理プログラムPとともに第2秘密鍵Ks2を通信ネットワーク8を経由して2次ユーザ端末装置5に供給する。

【0125】第2秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザは、暗号化データCmks2を著作権管理プログラムPを利用して第2秘密鍵Ks2を用いて復号化し

$M = D(Ks2, Cmks2)$

復号化されたデータMをそのままあるいは加工して利用する。

【0126】データMが2次ユーザ端末装置5内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、データMは著作権管理プログラムPにより第2秘密鍵Ks2によって暗号化される。

$Cmks2 = E(Ks2, M)$

【0127】この場合、さらに著作権管理プログラムPが、2次ユーザ端末装置5における著作権管理プログラムPの使用回数N2と秘密鍵Ks2に基づいて第3秘密鍵Ks3を生成するようにすることもできる。

$Ks3 = P(N2 + Ks2)$

この場合、データMが2次ユーザ端末装置5内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して3次ユーザ6に転送される場合には、データMは著作権管理プログラムPにより第3秘密鍵Ks3によって暗号化される。

$Cmks3 = E(Ks3, M)$

【0128】〔実施例8〕図4に示されたのは、データ著作権管理システムの実施例8のシステム構成であり、この実施例8において単一のデータベースから供給される原データはユーザからの要求に応じて双方向的に供給される。この実施例において採用される暗号方式は秘密鍵方式であり、第1秘密鍵に基づいて第2秘密鍵が生成される。

【0129】この図において、1はデータベース、4は1次ユーザ端末装置、5は2次ユーザ端末装置、6は3次ユーザ端末装置、7はn次ユーザ端末装置である。また、18は著作権管理センタ、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワークである。

【0130】これらのうちデータベース1、著作権管理

センタ18、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6及びn次ユーザ端末装置7は通信ネットワーク8によって相互に接続可能とされている。

【0131】このシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要がある。また、この登録の際にデータベース組織用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信ソフトウェアプログラムが含まれている。このデータベース組織用ソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマスクROM、EPROM、EEPROM等に格納することも可能である。

【0132】また、このシステムにおいてはユーザ側で秘密鍵を生成するためユーザ端末装置に秘密鍵生成アルゴリズムが格納されるが、この秘密鍵生成アルゴリズム自身は必ずしも秘密のものではないため、データベース組織に利用を登録するときにユーザに対して提供されるデータベース組織用ソフトウェアに内蔵させてもよい。なお、広告付等の無料で供給される原データの場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。

【0133】なお、この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、1点鎖線で示された経路は各データベースからの利用形態に対応した利用許可情報及び著作権管理プログラムとともに秘密鍵が転送される経路である。

【0134】この図において、データベース1にはテキストデータ、グラフィックスデータあるいはバイナリデータ、音声データ、映像データが暗号化されていない状態で保管されている。

【0135】1次ユーザは1次ユーザ端末装置4を使用して通信ネットワーク8を経由してデータベース1に対して、利用することを希望する原データ名を指定して原データM0の利用を申し込む。

【0136】1次ユーザ端末装置4から原データM0の利用申し込みを受けたデータベース1は、原データM0を第1秘密鍵Ks1で暗号化し、

$Cm0ks1 = E(Ks1, M0)$

暗号化された原データCm0ks1及び第1秘密鍵Ks1とともに著作権管理プログラムPを1次ユーザ端末装置4に供給する。この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムPにより、秘密鍵の生成及びデータの復号化/暗号化が行われる。なお、この暗号アルゴリズムを第1秘密鍵Ks1に依存するものにしておけば、著作権管理プログラムPをその原データM0に固有のものとすることができる。

【0137】第1秘密鍵Ks1を用いて暗号化された原データCm0ks1とともに第1秘密鍵Ks1と著作権管理プログラムPを受け取った1次ユーザ端末装置4は、第1秘密鍵Ks1を用いて暗号化原データCm0ks1を復号し、
 $M0 = D(Ks1, Cm0ks1)$

復号化された原データM0をそのままあるいは加工データM1として利用する。また、著作権管理プログラムPにより、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2が生成される。

$$Ks2 = P(Ks1)$$

【0138】復号された原データあるいは加工されたデータであるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、そのデータMは著作権管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0139】暗号化データCmks2は、原データ名あるいは原データ番号とともに、記録媒体11に複写され、あるいは、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0140】暗号化データCmks2を入手した2次ユーザは、2次ユーザ端末装置5を利用して、原データ名あるいは原データ番号を指定することにより原データあるいは加工データであるデータMの2次利用を著作権管理センタ18に申し込む。

【0141】データMの2次利用申込を受けた2次著作権管理センタ18は、原データ名あるいは原データ番号を手がかりとして第1秘密鍵Ks1を探し出し、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、
 $Ks2 = P(Ks1)$

生成された第2秘密鍵Ks2を著作権管理プログラムPとともに2次ユーザ端末装置5に供給する。

【0142】第2秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザ端末装置5は、暗号化データCmks2を著作権管理プログラムPを利用して第2秘密鍵Ks2を用いて復号化して
 $M = D(Ks2, Cmks2)$

復号化されたMをそのままあるいは加工して利用する。データMが2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、

【0143】著作権管理プログラムPにより第2秘密鍵Ks2に基づいて第3秘密鍵Ks3が生成され、
 $Ks3 = P(Ks2)$

著作権管理プログラムPによりこの生成された第3秘密鍵Ks3を用いてデータMが暗号化される。

$$Cmks3 = E(Ks3, M)$$

【0144】【実施例9】次に説明する実施例9は図4に示された実施例8と同様に単一のデータベースから供

給される原データはユーザからの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式であり、第2秘密鍵の生成に実施例8で用いられた第1秘密鍵に加えてユーザデータを利用する。なお、この実施例のシステム構成は実施例8のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【0145】データベース1には、原データM0が暗号化されていない状態で保管されている。1次ユーザが1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0146】データメニューが転送されると1次ユーザはデータメニュー検索を行い原データM0を選択し、選択した原データM0の原データ名等を指定することによりデータベース1に対して、原データM0の1次利用を申し込む。

【0147】1次ユーザ端末装置4から原データM0の利用申し込みを受けたデータベース1では、原データM0が読み出され、読み出された原データM0が第1秘密鍵Ks1で暗号化され、
 $Cm0ks1 = E(Ks1, M0)$

暗号化された原データCm0ks1及び第1秘密鍵Ks1とともに著作権管理プログラムPを1次ユーザ端末装置4に供給される。

【0148】ここで使用される著作権管理プログラムPは全てのデータベース組織において共通のものであり、さらに暗号アルゴリズムを有する暗号プログラムを含んでおり、この暗号プログラムにより暗号生成及びデータの復号化/暗号化が行われる。

【0149】第1秘密鍵Ks1と著作権管理プログラムPを受け取った1次ユーザ端末装置4は、著作権管理プログラムPにより第1秘密鍵Ks1を用いて暗号化された原データCm0ks1を復号化して
 $M0 = D(Ks1, Cm0ks1)$

復号化された原データM0をそのままあるいは加工データM1として利用する。また、著作権管理プログラムPが、1次ユーザ情報Iu1に基づいて第2の秘密鍵Ks2を生成する。

$$Ks2 = P(Iu1)$$

この第2の秘密鍵Ks2は、1次ユーザ情報Iu1以外に第1秘密鍵Ks1あるいは1次ユーザデータIu1と第1秘密鍵Ks1とに基づいて生成することもできる。

$$Ks2 = P(Ks1)$$

$$Ks2 = P(Ks1 + Iu1)$$

【0150】原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、そのデータMは著作権管理プログラムPにより第2の秘

10

20

30

40

50

密鍵Ks2によって暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0151】第2の秘密鍵Ks2によって暗号化されたデータCmks2は、原データ名あるいは原データ番号が付されるとともに、記録媒体11に複写されあるいは、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0152】第2秘密鍵Ks2によって暗号化されたデータCmks2を入手した2次ユーザは、2次ユーザ端末装置5を利用してデータMの2次利用を著作権管理センタ18に申し込むが、このときに原データ名あるいは原データ番号等を指定するとともに暗号化されていない1次ユーザ情報Iu1を提示する。

【0153】データMの2次利用申込を受けた著作権管理センタ18は、指定された原データ名あるいは原データ番号により第1秘密鍵Ks1を探し出し、著作権管理プログラムPにより提示された1次ユーザ情報Iu1、探し出された第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、著作権管理プログラムPとともに2次ユーザ端末装置5に供給する。

【0154】第2秘密鍵Ks2と著作権管理プログラムPを受け取った2次ユーザは2次ユーザ端末装置5を利用して、著作権管理プログラムPにより第2の秘密鍵Ks2を用いて暗号化されたデータCmks2を復号化して、

$$M = D(Ks2, Cmks2)$$

復号化されたデータMをそのままあるいは加工して利用する。データMが2次ユーザ端末装置5内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータMは著作権管理プログラムPにより第2の秘密鍵Ks2によって暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0155】なお、この場合、著作権管理プログラムPが、1次ユーザ情報Iu1、第2秘密鍵Ks2あるいは1次ユーザ情報Iu1と第2秘密鍵Ks2に基づいて第3の秘密鍵Ks3を生成する

$$Ks3 = P(Iu1)$$

$$Ks3 = P(Iu1 + Ks1)$$

$$Ks3 = P(Ks1)$$

ようにすることもできる。また、2次ユーザが2次利用申込を行うときに2次ユーザ情報Iu2を提示し、1次ユーザ情報Iu1の代わりに2次ユーザ情報Iu2に基づいて第3秘密鍵を生成することもできる。データMは著作権管理プログラムPにより第3秘密鍵Ks3によって暗号化される。

$$Cmks3 = E(Ks3, M)$$

【0156】この実施例において、第2秘密鍵Ks2を生成する著作権管理プログラムPは全データベース組織において共通のものであるから、どのデータベース組織においても、1次ユーザデータIu1及び第1秘密鍵Ks1が

変更されない限り同一の原データに対しては同一の第2秘密鍵Ks2が生成される。

【0157】【実施例10】次に説明する実施例10は図4に示された実施例8と同様に原データが単一のデータベースからユーザからの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式である。この実施例においては、第2秘密鍵の生成に実施例9で用いられたユーザ情報に代えて著作権管理プログラムの使用回数を利用する。なお、この実施例のシステム構成は実施例8のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【0158】データベース1には、原データM0が暗号化されていない状態で保管されている。1次ユーザが1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0159】データメニューが転送されると1次ユーザはデータメニュー検索を行い原データM0を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由してデータベース1に対して、原データ名等を指定して1次利用を希望する原データM0の利用を申し込む。

【0160】1次ユーザからデータ利用申し込みを受けたデータベース1は、原データM0を第1秘密鍵Ks1で暗号化し、

$$Cm0ks1 = E(Ks1, M0)$$

暗号化されたデータCm0ks1と第1秘密鍵Ks1とともに著作権管理プログラムPを1次ユーザ端末装置4に供給する。

【0161】この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、この暗号プログラムにより暗号鍵生成及びデータの復号化/暗号化が行われる。また、著作権管理プログラムPにはカウンタが付属しており、このカウンタがプログラムの使用回数Nあるいは原データの利用回数Nを計数する。なお、この暗号アルゴリズムを第1秘密鍵Ks1に依存するものにしておけば、著作権管理プログラムPをその原データ固有のものとして行うことができる。

【0162】第1秘密鍵Ks1と著作権管理プログラムPを受け取った1次ユーザは、暗号化された原データCm0ks1を著作権管理プログラムPを使用して第1秘密鍵Ks1を用いて復号化して、

$$M0 = D(Ks1, Cm0ks1)$$

復号化された原データM0をそのままあるいは加工データM1として利用する。

【0163】データの著作権を保護するため、原データM0あるいは加工データM1であるデータMが1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、そのデータMは著作権

10

20

30

40

50

管理プログラムPにより暗号化される。言い換えれば、これらの利用が行われるときには必ず著作権管理プログラムが動作する。

【0164】一方、供給された著作権管理プログラムPが使用されるとプログラム内のカウンタが計数を行い、そのカウント数Nと第1秘密鍵Ks1に基づいて著作権管理プログラムPが第2秘密鍵Ks2を生成する。

$$Ks2 = P(N + Ks1)$$

【0165】この第2秘密鍵Ks2は著作権管理プログラムPの使用回数Nにも基づいているため、データMは利 10 用される度に新しい第2秘密鍵Ks2で暗号化される。

$$Cmks2 = E(Ks2, M)$$

数後に生成された第2秘密鍵Ks2によって暗号化されたデータCmks2は、原データ名あるいは原データ番号、1次ユーザ情報Iu1及びカウンタデータNとともに、記録媒体11に複写あるいは、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0166】第2秘密鍵Ks2を用いて暗号化されたデータCmks2を入手した2次ユーザは、原データ名あるいは原データ番号、1次ユーザ情報Iu1及びカウンタデータ 20 Nを提示して、データMの2次利用を著作権管理センタ18に申し込む。

【0167】暗号化されたデータCmks2の2次利用申込を受けた著作権管理センタ18は、そのデータの原データ名あるいは原データ番号から第1の秘密鍵Ks1を探し出し、第1の秘密鍵、提示された1次ユーザ情報Iu1及びカウンタデータNから第2の秘密鍵Ks2を生成し、生成された第2の秘密鍵Ks2を著作権管理プログラムPとともに2次ユーザ端末装置5に転送する。

【0168】第2の秘密鍵Ks2と著作権管理プログラム 30 Pを受け取った2次ユーザ端末装置5は、著作権管理プログラムPを利用して暗号化データCmks2を第2の秘密鍵Ks2を用いて復号化し

$$M = D(Ks2, Cmks2)$$

復号化されたデータMをそのままあるいは加工して利用する。

【0169】データが2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、そのデータは著作権管理プログラムにより 40 第2の秘密鍵によって暗号化される。

【0170】なお、さらに著作権管理プログラムが、第2の秘密鍵に基づいて第3の秘密鍵を生成することもできる。

【0171】以上説明した実施例1から実施例10はいずれもデータベースから供給された単一原データを利用する場合についてのものである。しかし、データの利用形態としての加工には単一のデータを加工する他に、同一のデータベースから入手した複数の原データを組み合 50 わせて新しいデータを作成する場合及び複数のデータベ

ースから入手した複数の原データを組み合わせる新しいデータを作成する場合がある。

【0172】【実施例11】次に説明する実施例11

は、1次ユーザが単一のデータベースに保存されている複数の原データを組み合わせる新しいデータを作成する実施例であり、1次ユーザはデータベースに保存されている第1、第2、第3の原データを材料にして新しいデータを作成する。

【0173】この実施例においては図4に示された実施例8と同様に複数の原データが単一のデータベースからユーザの要求に応じて供給される。この実施例において採用される暗号方式は秘密鍵方式である。なお、この実施例のシステム構成は実施例8のシステム構成と異なる点はないので、システム構成についての説明は省略する。

【0174】データベース1には、原データM01、M02、M03が暗号化されていない状態で保管されている。1次ユーザが1次ユーザ端末装置4を利用してデータベース1にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【0175】データメニューが転送されると1次ユーザはデータメニュー検索を行い原データM01、M02、M03を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由してデータベース1に対して、第1、第2、第3の原データM01、M02、M03の原データ名あるいは原データ番号を指定して各原データの供給を申し込むがこのときに1次ユーザ情報Iu1を提示する。

【0176】1次ユーザから第1、第2、第3の原データM01、M02、M03の供給申し込みを受けたデータベース1は、供給申込を受けた第1、第2、第3の原データM01、M02、M03を各々第1、第2、第3の秘密鍵Ks01、Ks02、Ks03を用いて暗号化し、

$$Cm01ks01 = E(Ks01, M01)$$

$$Cm02ks02 = E(Ks02, M02)$$

$$Cm03ks03 = E(Ks03, M03)$$

第1、第2、第3の秘密鍵Ks01、Ks02、Ks03及び全てのデータベース組織と全ての原データに共通する著作権管理プログラムPを1次ユーザ端末装置4に供給する。この著作権管理プログラムPには暗号アルゴリズムを有する暗号プログラムが含まれており、暗号鍵生成及び復号化/暗号化が行われる。

【0177】暗号化第1原データCm01ks01、暗号化第2原データCm02ks02、暗号化第3原データCm03ks03、第1秘密鍵Ks01、第2秘密鍵Ks02、第3秘密鍵Ks03、著作権管理プログラムPを受け取った1次ユーザ端末装置4は、著作権管理プログラムPを利用してこれらの秘密鍵Ks01、Ks02、Ks03を用いて第1、第2、第3の各暗号化原データCm01ks01、Cm02ks02、Cm03ks03を復号化し

01=D (Ks01, Cm01ks01)

02=D (Ks02, Cm02ks02)

03=D (Ks03, Cm03ks03)

データM01, M02, M03を加工して新しいデータM1作成する。

【0178】また、著作権管理プログラムPが第1秘密鍵Ks01, 第2秘密鍵Ks02, 第3秘密鍵Ks03, 1次ユーザデータIulのうちの1つあるいはこの中のいくつかに基づいて第4秘密鍵Ks4を生成する。

$s4=P(Ks01/Ks02/Ks03/Iul)$

【0179】加工データM1が1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ5に転送される場合には、著作権管理プログラムPにより第4秘密鍵Ks4によって暗号化される。

$mks4=E(Ks4, M1)$

【0180】暗号化加工データCm1ks4は原データ名あるいは原データ番号及び1次ユーザデータIulとともに、記録媒体11に複写あるいは通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0181】暗号化加工データCm1ks4を入手した2次ユーザは2次ユーザ端末装置5を利用して暗号化加工データCm1ks4の2次利用を著作権管理センタ18に申し込むが、このときに原データM01, M02, M03のデータあるいはデータ番号等を指定するとともに1次ユーザ情報Iulを提示する。

【0182】2次ユーザから暗号化加工データCm1ks4の2次利用申込を受けた著作権管理センタ18は、第1データM01のデータ名あるいはデータ番号から第1秘密鍵Ks01を探し出し、第2原データM02のデータ名あるいはデータ番号から第2秘密鍵Ks02を探し出し、第3原データM03のデータ名あるいは原データ番号から第3秘密鍵Ks03を探し出し、共通の著作権管理プログラムPにより、探し出された第1秘密鍵Ks01, 第2秘密鍵Ks02, 第3秘密鍵Ks03, 1次ユーザ情報Iulのうちの1つあるいはこの中のいくつかに基づいて第4秘密鍵Ks4を生成し、

$s4=P(Ks01/Ks02/Ks03/Iul)$

共通の著作権管理プログラムPとともに2次ユーザ5に提供する。

【0183】第4の秘密鍵と共通の著作権管理プログラムを受け取った2次ユーザは、著作権管理プログラムPにより第4秘密鍵Ks4を用いて加工データM1を復号化し、

$M1=D(Ks4, Cm1ks4)$

復号化された加工データM1をそのままあるいは再加工データM2として利用する。

【0184】加工データM1あるいは再加工データM2が2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合あるいは通信ネットワーク8を経由

して3次ユーザ6に転送される場合には、著作権管理プログラムPにより第4秘密鍵Ks4に基づいて第5秘密鍵Ks5が生成され、

$s5=P(Ks4)$

それらのデータは著作権管理プログラムPにより第5秘密鍵Ks5を用いて暗号化される。

$mks5=E(Ks5, Cm1)$

$mks5=E(Ks5, Cm2)$

【0185】なお、共通の著作権管理プログラムPが、第4秘密鍵Ks4を用いて第5秘密鍵Ks5を生成し、生成された第5秘密鍵Ks5を用いて以後の暗号化/復号化を行うようにすることもできる。

【0186】この実施例において、第4の秘密鍵を生成する著作権管理プログラムは全データベース組織において共通のものであるから、どのデータベース組織においても、1次ユーザデータ及び第1の秘密鍵が変更されない限り同一の原データに対しては同一の第4の秘密鍵が生成される。

【0187】この実施例における、共通の著作権管理プログラムは著作権管理センタ18から供給されるが、各ユーザ端末装置内のROMに内蔵、あるいはデータベースを利用するためのソフトウェアに内蔵してもよい。

【0188】〔実施例12〕次に説明する実施例12では、複数のデータベースからユーザの要求に応じて供給される複数の原データを組み合わせて新しいデータを作成する実施例であり、この実施例においては暗号鍵方式として秘密鍵方式が採用される。

【0189】図5において、19, 20, 21はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、音声データあるいは映像データが格納された第1, 第2及び第3のデータベース、4は1次ユーザ端末装置、5は2次ユーザ端末装置、6は3次ユーザ端末装置、7はn次ユーザ端末装置、10はデータ著作権を管理する著作権管理センタであり、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等である通信ネットワークである。

【0190】これらのうち第1, 第2及び第3データベース19, 20, 21, 著作権管理センタ10, 1次ユーザ端末装置4, 2次ユーザ端末装置5, 3次ユーザ端末装置6及びn次ユーザ端末装置7は通信ネットワーク8によって相互に接続可能とされている。

【0191】このシステムを利用する各ユーザは予め各々のデータベース組織に登録しておく必要がある。また、この登録の際に各データベース組織の利用ソフトウェアがユーザに対して供給される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアプログラムが含まれている。これらのデータベース組織利用ソフトウェアは、ユーザ端末装置内の固定ディスクに格納してもよいが、ユーザ端末装置に内蔵されるマ

スクROM, EPROM, EEPROM等に格納することも可能である。

【0192】また、このシステムにおいてはユーザ側で秘密鍵を生成するためにユーザ端末装置に暗号鍵生成アルゴリズムが格納されるが、この暗号鍵生成アルゴリズム自身は必ずしも秘密のものではないため、各々のデータベース組織利用ソフトウェアに内蔵させてもよい。なお、広告付等の無料で供給される原データの場合には、暗号化を必要としない場合もあるが、その場合でも著作権は存在するため著作権を使用するための手続きは必要である。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置から各データベース及び著作権管理センタへ要求を行う経路であり、1点鎖線で示された経路は各データベース及び著作権管理センタから各ユーザ端末装置へ利用形態に対応する許可情報、著作権管理プログラム及び暗号鍵が転送される経路である。

【0193】この実施例においては原データ毎に異なる秘密鍵及び著作権管理プログラムが使用されるが、これらは予め各データベース及び著作権管理センタに保管されている。

【0194】第1データベース19には、第1原データM1が暗号化されていない状態で保管されており、1次ユーザが1次ユーザ端末装置4を利用して第1データベース19にアクセスすると、データメニューが転送される。

【0195】データメニューが転送されると1次ユーザはデータメニュー検索を行い第1原データM1を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由して第1データベース19に対して、原データ名あるいは原データ番号を指定して第1原データM1の供給を申し込むがこのときに1次ユーザ情報Iu1を提示する。

【0196】1次ユーザから第1原データM1の利用申し込みを受けた第1データベース19は、利用申込を受けた第1の原データM1を第1秘密鍵Ks1を用いて暗号化し、

$$Cm1ks1 = E(Ks1, M1)$$

1次ユーザ端末装置4に供給する。

【0197】第2データベース20には、第2原データM2が暗号化されていない状態で保管されており、1次ユーザが1次ユーザ端末装置4を利用して第2データベース20にアクセスすると、データメニューが転送される。

【0198】データメニューが転送されると1次ユーザはデータメニュー検索を行い第2原データM2を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由して第2データベース20に対して、原データ名あるいは原データ番号を指定して第2原データM2の供給を申し込むがこのときに1次ユーザ情報Iu1を提

示する。

【0199】1次ユーザから第2原データM2の利用申し込みを受けた第2データベース20は、利用申込を受けた第2原データM2を第2秘密鍵Ks2を用いて暗号化し、

$$Cm2ks2 = E(Ks2, M2)$$

1次ユーザ端末装置4に供給する。

【0200】第3データベース21には、第2原データM3が暗号化されていない状態で保管されており、1次ユーザが1次ユーザ端末装置4を利用して第3データベース21にアクセスすると、データメニューが転送される。

【0201】データメニューが転送されると1次ユーザはデータメニュー検索を行い第3原データM3を選択し、1次ユーザ端末装置4を利用して、通信ネットワーク8を経由して第3データベース22に対して、原データ名あるいは原データ番号を指定して第3原データM3の供給を申し込むがこのときに1次ユーザ情報Iu1を提示する。

【0202】1次ユーザから第3原データM3の利用申し込みを受けた第3データベース21は、利用申込を受けた第3原データM3を第3秘密鍵Ks3を用いて暗号化し、

$$Cm3ks3 = E(Ks3, M3)$$

1次ユーザ端末装置4に供給する。

【0203】暗号化第1、第2、第3原データCm1ks1、Cm2ks2、Cm3ks3を供給された1次ユーザは、1次ユーザ端末装置4を利用して暗号化第1、第2、第3の原データCm1ks1、Cm2ks2、Cm3ks3を1次利用するために通信ネットワーク8を経由して、原データ名あるいは原データ番号を指定して、著作権管理センタ10に対して1次利用申込を行う。

【0204】1次ユーザからの暗号化第1、第2、第3原データCm1ks1、Cm2ks2、Cm3ks3の1次利用申し込みを受けた著作権管理センタ10は、第1原データM1の暗号鍵である第1秘密鍵Ks1とともに第1著作権管理プログラムP1、第2原データM2の暗号鍵である第2秘密鍵Ks2とともに第2著作権管理プログラムP2、第3原データM3の暗号鍵である第3秘密鍵Ks3とともに第3著作権管理プログラムP3を1次ユーザ端末装置4に供給する。

【0205】これらの著作権管理プログラムP1、P2、P3には暗号アルゴリズムを有する暗号プログラムが各々含まれており、これらの暗号プログラムにより新しい秘密鍵の生成及びデータの復号/暗号化が行われる。なお、これらの暗号アルゴリズムを各々第1、第2、第3秘密鍵Ks1、Ks2、Ks3に依存するものにしておけば、第1、第2、第3著作権管理プログラムP1、P2、P3を各第1、第2、第3原データM1、M2、M3に固有のものとする事ができる。

【0206】第1, 第2, 第3の秘密鍵Ks1, Ks2, Ks3を受け取った1次ユーザ端末装置4は、これらの秘密鍵を用いて暗号化された第1, 第2, 第3の各原データCm1ks1, Cm2ks2, Cm3ks3を復号化して、

M1=D (Ks1, Cm1ks1)

M2=D (Ks2, Cm2ks2)

M3=D (Ks3, Cm3ks3)

復号化された各原データM1, M2, M3をそのままあるいは加工して利用する。また、第1著作権管理プログラムP1が第1秘密鍵Ks1に基づいて第4の秘密鍵Ks4を、第2著作権管理プログラムP2が第2秘密鍵Ks2に基づいて第5秘密鍵Ks5を、第3著作権管理プログラムP3が第3の秘密鍵Ks3に基づいて第6秘密鍵Ks6を、

Ks4=P1 (Ks1)

Ks5=P2 (Ks2)

Ks6=P3 (Ks3)

【0207】各原データM1, M2, M3あるいは加工データM4, M5, M6が1次ユーザ端末装置4内に保存される場合、記録媒体11に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置5に転送される場合には、第1の原データM1あるいは加工データM4が第1著作権管理プログラムP1により第4秘密鍵Ks4を用いて、第2の原データM2あるいは加工データM5が第2著作権管理プログラムP2により第5秘密鍵Ks5を用いて、第3の原データM3あるいは加工データM6が第3著作権管理プログラムP3により第6秘密鍵Ks6を用いて、各々暗号化される。

Cm1ks4=E (Ks4, M1)

Cm2ks5=E (Ks5, M2)

Cm3ks6=E (Ks6, M3)

Cm4ks4=E (Ks4, M4)

Cm5ks5=E (Ks5, M5)

Cm6ks6=E (Ks6, M6)

【0208】第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6によって暗号化された原データCm1ks4, Cm2ks5, Cm3ks6あるいは暗号化された加工データCm4ks4, Cm5ks5, Cm6ks6は第1, 第2, 第3の原データ名あるいは原データ番号及び1次ユーザデータIu1とともに、記録媒体11に複写されて、あるいは通信ネットワーク8を経由して2次ユーザ端末装置5に転送される。

【0209】暗号化された第1, 第2, 第3の原データCm1ks4, Cm2ks5, Cm3ks6あるいは暗号化された加工データCm4ks4, Cm5ks5, Cm6ks6を供給された2次ユーザ端末装置5においては、原データ名あるいは原データ番号を指定することにより、第1, 第2, 第3の原データM1, M2, M3あるいは加工データMの2次利用を著作権管理センタ10に申し込む。

【0210】2次ユーザ端末装置5から第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M

5, M6の2次利用申込を受けた著作権管理センタ10は、第1の原データ名から第1秘密鍵Ks1及び第1著作権管理プログラムP1を探し出し、第2の原データ名あるいは原データ番号から第2秘密鍵Ks2及び第2著作権管理プログラムP2を探し出し、第3の原データ名から第3秘密鍵Ks3及び第3著作権管理プログラムP3を探し出し、第1著作権管理プログラムP1が第1秘密鍵Ks1から第4秘密鍵Ks4を生成し、第2著作権管理プログラムP2が第2秘密鍵Ks2から第5秘密鍵Ks5を生成し、第3著作権管理プログラムP3が第3秘密鍵から第6の秘密鍵Ks6を生成し、

Ks4=P1 (Ks1)

Ks5=P2 (Ks2)

Ks6=P3 (Ks3)

第1, 第2, 第3の著作権管理プログラムP1, P2, P3とともに2次ユーザ端末装置5に供給する。

【0211】第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6と第1, 第2, 第3著作権管理プログラムP1, P2, P3を受け取った2次ユーザ端末装置5では、暗号化された第1の原データCm1ks4あるいは加工データCm4ks4が第1著作権管理プログラムP1により第4秘密鍵Ks4を用いて、暗号化された第2の原データCm2ks5あるいは加工データCm5ks5が第2著作権管理プログラムP2により第5秘密鍵Ks5を用いて、暗号化された第3の原データCm3ks6あるいは加工データCm6ks6が第3著作権管理プログラムP3により第6秘密鍵Ks6を用いて、各々復号化され、

M4=D (Ks4, Cm4ks4)

M5=D (Ks5, Cm5ks5)

M6=D (Ks6, Cm6ks6)

復号化された各データM4, M5, M6をそのままあるいは加工して利用する。

【0212】第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M5, M6が2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して2次ユーザ端末装置6に転送される場合には、第1の原データM1あるいは加工データM4は第1著作権管理プログラムP1により第4秘密鍵Ks4を用いて、第2の原データM2あるいは加工データM5は第2著作権管理プログラムP2により第5秘密鍵Ks5を用いて、第3の原データM3あるいは加工データM6は第3著作権管理プログラムP3により第6秘密鍵Ks6を用いて、各々暗号化される。

【0213】なお、この場合第1著作権管理プログラムP1が第4秘密鍵Ks4に基づいて第7秘密鍵Ks7を、第2著作権管理プログラムP2が第5秘密鍵Ks5に基づいて第8秘密鍵Ks8を、第3著作権管理プログラムP3が第6秘密鍵Ks6に基づいて第9秘密鍵Ks9を各々生成するようにし、

Ks7=P1 (Ks4)

$Ks8 = P2 (Ks5)$

$Ks9 = P3 (Ks6)$

これら第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M5, M6が2次ユーザ端末装置5内に保存される場合、記録媒体12に複写される場合、通信ネットワーク8を経由して3次ユーザ端末装置6に転送される場合には、それら第1, 第2, 第3の原データM1, M2, M3あるいは加工データM4, M5, M6は第1, 第2, 第3著作権管理プログラムP1, P2, P3により第7, 第8, 第9秘密鍵Ks7, Ks8, Ks9を用いて暗号化されるようにすることもできる。

$Cm1ks7 = E (Ks7, M1)$

$Cm2ks8 = E (Ks8, M2)$

$Cm3ks9 = E (Ks9, M3)$

$Cm4ks7 = E (Ks7, M4)$

$Cm5ks8 = E (Ks8, M5)$

$Cm6ks9 = E (Ks9, M6)$

【0214】[実施例13] 次に説明する実施例13は、実施例12と同様に複数のデータベースからユーザの要求に応じて供給される複数の原データを利用して新しいデータを作成する実施例であり、この実施例においては暗号鍵方式として秘密鍵方式が採用される。また、暗号化/復号化に用いられる暗号鍵の生成に実施例7及び実施例11の場合と同様にさらに著作権管理プログラムの使用回数が利用される。

【0215】この実施例においては、著作権管理プログラムにはカウンタが付属しており、このカウンタがプログラムの使用回数あるいは原データの利用回数を計数し、そのカウンタ数Nを利用して第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6が生成される。2次ユーザは各々の原データの原データ名あるいは原データ番号、1次ユーザデータとともにカウンタ数Nを提示して、データの2次利用を著作権管理センタ10に申し込む。データの2次利用申込を受けた著作権管理センタ10は、各々の原データ名あるいは原データ番号から第1, 第2, 第3秘密鍵Ks1, Ks2, Ks3を探し出し、第1, 第2, 第3著作権管理プログラムP1, P2, P3により各々のデータの第1, 第2, 第3秘密鍵Ks1, Ks2, Ks3, 1次ユーザIu1及び第1, 第2, 第3カウンタ数N1, N2, N3から第4, 第5, 第6秘密鍵Ks4, Ks5, Ks6を生成し、第4, 第5, 第6著作権管理プログラムP1, P2, P3とともに2次ユーザに提供する。これ以外の点は、実施例12のシステム構成と異なる点はないので具体的な説明は省略する。

【0216】[実施例14] 1次ユーザが入手した原データをそのまま複写して2次ユーザに供給した場合にはそのデータに何等の価値も加えられていないため、そのデータに1次ユーザの著作権は発生しない。しかし、入手した原データから新しいデータを作成した場合、すなわち、入手した単一の原データから新しいデータを作成

した場合及び入手した複数の原データから新しいデータを作成した場合には、新しいデータについて1次ユーザの2次的著作権が発生する。

【0217】一方、加工に利用された原データにも著作権者の著作権が存在しているため、加工データには原データの著作権者の著作権と加工を行った1次ユーザの2次的著作権とが存在することになる。著作権は単なる物権ではなく人格権の要素が強い権利であるため、著作権者がその存在を強く主張することが多い。そのため、原データの加工が行われた場合であっても、加工データから原データあるいは著作権者を容易に特定できるようにすることが望ましい。

【0218】これまでに実施例1～13で説明したデータ著作権管理システムでは、原データあるいは加工データを暗号化することによってデータの著作権を管理しているが、このシステムではデータが原データであるのかあるいは加工データであるのか、また、加工データの中でどの部分が原データであり、どの部分が加工データであるのかは区別されることなくデータの著作権が管理されるため、加工データから原データあるいは著作権者を特定することはできない。

【0219】これから説明する実施例14ではデータを著作権しか存在しない原データと著作権に加えて2次的著作権も存在する加工データを区別できるとともに、原著作権と2次的著作権を明確に管理することができる。

【0220】データの加工は加工用プログラムを利用して原データに改変を加えることによってなされるため、原データと加工内容（必要な場合はさらに加工用プログラム）が特定されることによって加工データが再現される。いいかえれば、原データと加工内容（必要な場合はさらに加工用プログラム）が特定されなければ加工データの再現は不可能である。実施例14で説明する2次的著作権の管理は、原データと加工内容（必要な場合はさらに加工用プログラム）を特定し、これらを管理することによって行われる。

【0221】単一の原データにより新しいデータを作成する場合には、原データAを改変して加工データ

「A'」を得る場合、原データAに1次ユーザがデータXを付加することにより加工データ「A+X」を得る場合、原データAを原データ要素A1, A2, A3・・・に分割し配列をA3, A2, A1のように変更して加工データ「A''」を得る場合、原データAを原データ要素A1, A2, A3・・・に分割し1次ユーザのデータXをX1, X2, X3・・・に分割しこれらを配列して加工データ「A1+X1+A2+X2+A3+X3・・・」を得る場合等がある。これらの場合、原データの改変、原データの配列変更、原データと1次ユーザデータの組み合わせ、原データの分割及び1次ユーザデータとの組み合わせ、が各々2次的著作権の対象となり、これらの2次的著作権

権を保護する必要がある。なお、1次ユーザが付加したデータXには1次ユーザの著作権が存在することはいうまでもない。

【0222】複数の原データを組み合わせることにより新しいデータを作成する場合には、原データA、B、C・・・を単純に組み合わせて加工データ「A+B+C・・・」を得る場合、原データA、B、C・・・に1次ユーザがデータXを付加することにより加工データ「A+X」を得る場合、原データA、B、C・・・を原データ要素A1、A2、A3・・・、B1、B2、B3・・・、C1、C2、C3・・・に分割し組み合わせて配列を変更し加工データ「A1+B1+C1+・・・+A2+B2+C2+・・・+A3+B3+C3+・・・」を得る場合、原データA、B、C・・・を原データ要素A1、A2、A3・・・、B1、B2、B3・・・、C1、C2、C3・・・に分割し1次ユーザのデータX1、X2、X3・・・を組み合わせる配列を変更して加工データ「A1+B1+C1+X1+・・・+A2+B2+C2+X2+・・・+A3+B3+C3+X3+・・・」を得る場合等がある。これらの場合も、複数の原データの組み合わせ、複数の原データと1次ユーザデータの組み合わせ、複数の原データの分割及び配列変更、分割された複数の原データと1次ユーザデータの組み合わせ、が各々2次的著作権の対象となり、これらの2次的著作権を保護する必要がある。また、1次ユーザが付加したデータX1、X2、X3・・・には1次ユーザの著作権が存在することはいうまでもない。

【0223】図6に示されたのは複数の原データA、B、Cを利用して新しいデータDを作成する手法例である。この手法は原データA、B、Cから要素a、b、cを抽出(カット)し、抽出された要素a、b、cを貼り付けて(ペースト)1つのデータDを合成するカットアンドペースト手法によってデータの加工を行うものである。

【0224】ところで、原データ及び1次ユーザデータがデータであることは明白であるが、データの加工過程である原データの改変、原データの配列変更、原データと1次ユーザデータの組み合わせ、原データの分割及び1次ユーザデータとの組み合わせ、複数の原データの組み合わせ、複数の原データと1次ユーザデータの組み合わせ、複数の原データの分割及び配列変更、分割された複数の原データと1次ユーザデータの組み合わせもデータそのものである。

【0225】これまでに説明した実施例1～13では、データの著作権を原データあるいは加工データを暗号化することによってデータそのものの著作権を管理しているがこの他に、原データの配置関係及び加工手順等であるデータの加工過程もデータであることに着目すると、加工データに関する2次的著作権を原データに関する原作者の1次著作権及び1次ユーザデータに関する1次ユーザの1次著作権に加えて加工過程データに関する1

次ユーザの1次著作権を管理することによって保護することが可能となる。なお、加工過程や加工用プログラムを加工シナリオと呼ぶこともできる。

【0226】すなわち、加工データを原データと1次ユーザデータと加工過程データとから構成するものとし、これらの原データ、1次ユーザデータ及び加工過程データを各々これまでに実施例1～13で説明したデータ著作権管理システムによって管理することにより、原データとともに加工データの著作権を充分に管理することができる。なお、この場合データの加工において使用された加工用プログラムも必要ならばデータ著作権管理システムの管理対象とする。

【0227】このデータの加工は原データをその原データに対応する加工プログラムを使用して加工することもできるが、原データを最近注目されているオブジェクト指向ソフトウェアとして取り扱うようにすれば、より容易な加工とよりよいデータ著作権管理を行うことができる。また、さらに進んでエージェント指向ソフトウェアを採用すれば、ユーザは労することなくデータの合成を行うことができる。

【0228】エージェント指向ソフトウェアは、自律性・適応性・協調性を兼ね備えたプログラムであり、従来のソフトウェアのようにすべての作業手順を具体的に指示しなくても、ユーザの一般的な指示のみに基づいてその自律性・適応性・協調性との特質により、ユーザの要求に応えることができる。このエージェントプログラムをデータ著作権管理システムの基本的なシステムの中に組み込み、ユーザのデータベース利用形態を監視させ、その結果得られた情報をデータベース側あるいは著作権管理センタ側で収集するように構成することにより、ユーザのデータベース利用傾向をデータベース側あるいは著作権管理センタ側が知ることができ、よりきめの細かい著作権管理を行うことができる。したがって、エージェントプログラム及びデータも著作権保護の対象となり、原データと同様に暗号化される。

【0229】〔実施例15〕著作物中には、著作権が存在しないものと著作権が存在するものがあり、著作権が存在するものの中には、著作権の行使が行われるものと著作権の行使が行われないものがある。著作権が存在しない著作物としては法令によって著作権が存在しないものとされている著作物と著作権の期限が過ぎてしまったものがある。これらの著作権が存在しない著作物を除くすべての著作物には著作権が存在するが、著作権が存在する著作物には通常著作権の存在を主張する表示がなされており、この表示があることによって著作権の侵害に対する抑止効果が発揮される。このことは、著作物がデータである場合にも同様であって、著作権が存在するデータの場合には利用されるデータあるいはデータのファイルヘッダに著作権表示あるいは著作権者表示が行われることによってデータ著作権の侵害行為が抑止され

る。また、データに著作権が存在することを示す著作権フラグをファイルに付加し、ユーザ端末装置においてこのフラグを識別するようにすることにより、データ著作権の侵害行為を阻止することができる。

【0230】しかしながら、このような著作権に関する表示がなされていたとしてもそのデータ著作物を利用するユーザが著作権の存在を無視した場合には著作権の侵害が行われる可能性がある。そのような場合に対処するために、これまで説明した実施例においてはデータを暗号化し、暗号化データを復号化するための復号鍵を管理し、復号化データが保存、複写、転送される場合には復号鍵とは異なる暗号鍵を用いて暗号化／復号化が行われる。そのような場合であっても、ユーザ端末装置の主記憶装置上にデータが存在している状態においてデータをユーザ端末装置の主記憶装置以外の記憶装置に転送することにより、復号鍵と異なる暗号鍵を用いることなくデータを保存、複写、転送する可能性を完全に否定することはできない。

【0231】このような事態を防止するには、データ著作権利用ソフトウェアをユーザ端末装置の基本システムに組み込み、著作権行使の対象であるデータ著作物のファイルには著作権行使の属性を表示し、データ著作物の著作権行使属性についてユーザ端末装置の基本システムが監視し、著作権行使属性を有するデータ著作物はデータ著作権利用ソフトウェアによって管理されるようにすることが最善である。基本システムとしては、ユーザ端末装置がパーソナルコンピュータ等のコンピュータである場合にはDOS等のソフトウェアオペレーティングシステムであり、ユーザ端末装置が携帯情報端末装置あるいはSTB（セットトップボックス）である場合にはROMに内蔵されたハードウェアオペレーティングシステムである。なお、このオペレーティングシステムによるデータ著作権管理をより強固なものとするためには、データ著作権利用ソフトウェアはオペレーティングシステムのできるだけ上位のレベルに組み込むことが望ましい。

【0232】ユーザ端末装置の内部における処理及びデータはすべてオペレーティングシステムの管理下におかれている。言い換えれば、オペレーティングシステムはユーザ端末装置の内部における処理及びデータをすべて把握することができる。したがって、ユーザの指示によるのではなくオペレーティングシステムが把握したデータの利用状況に応じて著作権管理プログラムが自動的にデータ著作権の管理を行うようにすることができ、このような構成によればユーザによるデータ著作権の利用が容易になるとともに、より完全なデータ著作権管理を行うことができる。また、暗号鍵、データ著作権情報あるいは著作権ラベル等を管理する著作権管理プログラムはオペレーティングシステム自体が管理するシステム領域言い換えればユーザプログラムがアクセスすることがで

きないシステム領域に保持されることが望ましい。

【0233】しかし、この場合でもデータ著作物の一部のみが切りとられて利用されたような場合にはデータ著作権の管理が著しく困難になる。したがって、そのような状況をオペレーティングシステムが認識した場合には著作権管理プログラムにより切りとられた一部のデータに原データが有していた著作権情報及び著作権行使属性を付与するように構成することにより、切りとられた一部のデータのデータ著作権も管理する事が可能となる。また、切り取られたデータに元のデータ著作物の著作権を継承させるために、著作権管理プログラムによりその切り取られたデータと元のデータ著作物との間に親子関係のリンクを形成する。このようにしておけばユーザが複数の著作権付きデータからそれぞれ希望する部分を切り出して取り込み新しいデータを作成した場合にも、その新しいデータに元の各データ著作物の著作権を継承させることができる。

【0234】【実施例16】著作権は財産権の一種であるから、著作権を利用する場合には当然のこととして使用料支払いの問題が発生する。また、秘密鍵の提供、著作権管理プログラムの提供等のサービスは有料で行われる必要がある。これらの料金支払の最も簡易な方法は請求書の発行と支払を組み合わせたものであるが、この方法は使用料の支払が直接に行われる反面、作業が煩雑な上、不払い等の事故の可能性もある。また、通信回線事業者が行う料金徴収代行方法もあり、この方法は料金徴収作業を通信回線事業者が行うため簡便であり、不払い等の事故の可能性が低い反面、使用料の徴収が直接に行われないため、料金徴収代行手数料の支払が必要となる。

【0235】これらの問題を解決する方法として、デジタルキャッシュを利用する方法がある。このデジタルキャッシュはデジタルデータであり、暗号化され使用される。

【0236】【実施例17】さらに、以上説明したデータ著作権管理システムの構成はデータの流通だけではなくデジタルキャッシュの流通に対しても適用可能である。これまでに種々提案されているデジタルキャッシュシステムは秘密鍵方式で暗号化デジタルキャッシュデータを銀行預金口座あるいはクレジット会社のキャッシングサービスから転送してICカードに保存しており、入出力用の端末装置を利用して支払を行う。このICカードを電子財布として利用するデジタルキャッシュシステムは商店等入出力用の端末装置が設置されている場所であればどこでも使用可能である反面、入出力用の端末装置がない場所、例えば家庭等、では使用不可能である。

【0237】ところで、デジタルキャッシュは暗号化データであるからICカード以外にも暗号化データを保存することができ、かつ支払先にデータを転送すること

ができる装置であればどのようなものでもデジタルキャッシュデータを保存する電子財布として利用することができる。具体的に電子財布として利用可能なユーザ端末装置としては、パーソナルコンピュータ、インテリジェントテレビジョン装置、携帯情報端末装置 (Personal Digital Assistant PDA)、PHS (Personal Handyphone System) 等の携帯電話器、インテリジェント電話機、入出力機能を有するPCカード等がある。

【0238】このような端末装置をデジタルキャッシュ用の電子財布として利用することによる取引は、これまでに説明したデータ著作権管理システムの構成におけるデータベース1を顧客側銀行に、1次ユーザ端末装置4を顧客に、2次ユーザ端末装置5を小売店に、著作権管理センタ18を小売店側銀行に、3次ユーザ端末装置6を卸売またはメーカに置き換えることにより実現される。

【0239】また、デジタルキャッシュは単なるデータではなくデータと機能が結びついたオブジェクト (object) として処理されることが望ましい。デジタルキャッシュの取り扱いにおいては共通のデジタルキャッシュフォーム、所有者固有の未記入デジタルキャッシュフォーム、所有者固有のデジタルキャッシュフォームの書き込み欄、金額であるデジタルキャッシュデータ、デジタルキャッシュ取り扱いの指示、金額が書き込まれた所有者固有のデジタルキャッシュフォームがある。一方、オブジェクト指向プログラミング (object-oriented programming) においては、オブジェクト、クラス (class)、スロット (slot)、メッセージ (message)、インスタンス (instance) との概念が使用される。これらの対応関係は、共通のデジタルキャッシュフォームがオブジェクトとなり、所有者固有の未記入デジタルキャッシュフォームがクラスとなり、所有者固有のデジタルキャッシュフォームの記入欄がスロットとなり、デジタルキャッシュ取り扱いの指示がメッセージとなり、金額が記入された所有者固有のデジタルキャッシュフォームがインスタンスとなる。金額等からなるデジタルキャッシュデータは引数 (argument) として使用され、メッセージによりインスタンス変数 (instance variable) とも呼ばれるスロットに引き渡されて格納されることにより、金額等が更新されたデジタルキャッシュである新しいインスタンスが作られる。

【0240】オブジェクト化されたデジタルキャッシュについて、図6を用いて具体的に説明する。この図において、23、25、27は顧客端末装置に保存されている金額が書き込まれた顧客固有のデジタルキャッシュフォーム、29は小売店端末装置に保存されている金額が記入された小売店固有のデジタルキャッシュフォーム、24、26、28は各々の顧客の取引銀行にある預金口座である。

【0241】顧客23はデジタルキャッシュを使用す

るために、預金口座24から必要な金額を引き出し、端末装置に保存されているデジタルキャッシュフォーム23にデジタルキャッシュ引出金データ31を引き渡す。この場合、デジタルキャッシュフォーム23にはデジタルキャッシュ残金データ30が既に記入されているのが普通であるため、デジタルキャッシュフォーム23はクラスではなくインスタンスである。デジタルキャッシュ引出金データ31はデジタルキャッシュ残金データ30に対して加算することを指示するメッセージによりデジタルキャッシュフォーム23の記入欄であるスロットに引数として引き渡され、デジタルキャッシュフォーム23のデジタルキャッシュ残金データ30にデジタルキャッシュ引出金データ31が加算されてデジタルキャッシュフォーム23の記入欄の金額が変更された新しいインスタンスが作られる。

【0242】顧客が小売店に対して支払を行う場合には、支払金額に相当するデジタルキャッシュ支払金データ32をデジタルキャッシュフォーム23の記入欄の金額から減算することを指示するメッセージによりデジタルキャッシュフォーム記入欄であるスロットに引数として引き渡され、デジタルキャッシュフォーム23のデジタルキャッシュ残金データ30及びデジタルキャッシュ引出金データ31からデジタルキャッシュ支払金データ32が減算されてデジタルキャッシュフォーム23の記入欄の金額が変更された新しいインスタンスが作られる。また、デジタルキャッシュ支払金データ32が小売店固有のデジタルキャッシュフォーム29に引き渡される。

【0243】同様な引出処理及び支払処理が他の顧客のデジタルキャッシュフォーム25及び27でも行われ、デジタルキャッシュフォーム25からはデジタルキャッシュ支払金データ33が、デジタルキャッシュフォーム27からはデジタルキャッシュ支払金データ34が小売店固有のデジタルキャッシュフォーム29に引き渡される。小売店固有のデジタルキャッシュフォーム29の場合にもデジタルキャッシュ残金データ35が既に記入されているのが普通である。デジタルキャッシュ支払金データ32、デジタルキャッシュ支払金データ33及びデジタルキャッシュ支払金データ34はデジタルキャッシュ残金データ35に対して加算することを指示するメッセージによりデジタルキャッシュフォーム29の記入欄であるスロットに引数として引き渡され、デジタルキャッシュ残金データ35にデジタルキャッシュ支払金データ32、デジタルキャッシュ支払金データ33及びデジタルキャッシュ支払金データ34が加算されて、デジタルキャッシュフォーム記入欄の金額が変更された新しいインスタンスが作られる。

【0244】通常のオブジェクト指向プログラミングにおいては、引数がメッセージによりスロットに引き渡さ

れることにより新しいインスタンスが作られ、新しく作られたインスタンス全体引き渡されることはない。しかし、デジタルキャッシュの場合には安全上暗号技術が使用されるから、支払元においてデジタルキャッシュ支払金データが記入されたインスタンスを作り、このインスタンスを暗号化して支払先に引き渡すこともできる。

【0245】デジタルキャッシュを通信ネットワークを経由して転送することにより行われる取引システムの実施例を図7を用いて説明する。この実施例は図4に示されたシステム構成を利用したものであり、この図において、36は顧客、37は顧客36の取引銀行、38は小売店、39は小売店38の取引銀行、40はメーカ、41はメーカ40の取引銀行、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信ネットワークであり、顧客36、顧客の取引銀行37、小売店38、小売店の取引銀行39、メーカ40及びメーカの取引銀行41は通信ネットワーク8によって相互に接続可能とされている。このシステムにおいて、顧客36は銀行の他にキャッシングサービスを行うクレジット会社を利用することが可能であり、小売店とメーカとの間に適当な数の卸売り店を介在させることが可能である。また、42及び43はデジタルキャッシュデータが格納されるICカードあるいはPCカードであり、通信ネットワークを利用しない場合に使用される。なお、この図において、破線で示されたのは暗号化されたデジタルキャッシュデータの経路であり、実線で示されたのは顧客、小売店あるいはメーカから銀行への要求の経路であり、1点鎖線で示されたのは各銀行からの秘密鍵の経路である。さらに、この実施例では暗号鍵として顧客側銀行37が用意する第1秘密鍵及び顧客が生成する第2秘密鍵、小売店が生成する第3秘密鍵及びメーカが生成する第4秘密鍵が用いられる。この実施例では顧客側銀行37、小売店側銀行39、メーカ側銀行41を別個のものとして説明したが、これらを一括して金融システムとして考えてもよい。

【0246】デジタルキャッシュデータを暗号化／復号化するデジタルキャッシュ管理プログラムPは顧客36に予め配布され、ユーザ端末装置に保存されている。また、デジタルキャッシュ管理プログラムPは銀行との取引が行われる毎にデータとともに転送されるようにすることもできる。さらに、デジタルキャッシュ管理プログラムPは全銀行において共通するものとしてことが望ましい。顧客36はユーザ端末装置を利用して通信ネットワーク8を経由して金額を指定することにより、顧客側銀行37に預金口座からの預金の引出の申込を行うがこのときに顧客36の顧客情報Icを提示する。

【0247】顧客36から預金引出の申込を受けた顧客

側銀行37は、第1秘密鍵Ks1を選択あるいは作成し、引出金額のデジタルキャッシュデータM0をこの第1秘密鍵Ks1で暗号化し、

$$Cm0ks1 = E(Ks1, M0)$$

暗号化デジタルキャッシュデータCm0ks1及び復号鍵である第1秘密鍵Ks1を顧客36に転送するとともに、顧客情報Ic及び第1秘密鍵Ks1を保管する。この場合、第1秘密鍵Ks1は顧客側銀行37が予め用意したものから選択してもよいが、顧客が引き出し時に顧客情報Icを提示し、デジタルキャッシュ管理プログラムPにより、提示された顧客情報Icに基づいて作成することもできる。

$$Ks1 = P(Ic)$$

このようにすれば、第1秘密鍵Ks1を顧客36に固有のものとするだけでなく、顧客36に対して第1秘密鍵Ks1を転送する必要がないため、システムの安全性が高くなる。また、第1秘密鍵Ks1は顧客側銀行37の銀行情報Ibsあるいは銀行情報Ibsと作成日時に基づいて作成することもできる。

【0248】暗号化デジタルキャッシュデータCm0ks1及び第1秘密鍵Ks1を転送された顧客36は、デジタルキャッシュ管理プログラムPにより、顧客情報Ic、第1秘密鍵Ks1の何れか1つあるいは双方に基づいて第2秘密鍵Ks2を生成し、

$$Ks2 = P(Ic)$$

生成された第2秘密鍵Ks2がユーザ端末装置内に保存される。また、顧客36はデジタルキャッシュ管理プログラムPにより暗号化デジタルキャッシュデータCm0ks1を第1秘密鍵Ks1を用いて復号化して

$$M0 = D(Ks1, Cm0ks1)$$

内容を確認するが、内容が確認された復号化デジタルキャッシュデータM0が電子財布であるユーザ端末装置内に保存される場合には、生成された第2秘密鍵Ks2を用いてデジタルキャッシュ管理プログラムPにより暗号化される。

$$Cm0ks2 = E(Ks2, M0)$$

また、このときに第1秘密鍵Ks1が廃棄される。

【0249】小売店38から物品の購入を希望する顧客36は、デジタルキャッシュ管理プログラムPにより電子財布であるユーザ端末装置に保存されている暗号化デジタルキャッシュデータCm0ks2を第2秘密鍵Ks2を用いて復号化し、

$$M0 = D(Ks2, Cm0ks2)$$

必要な金額に対応するデジタルキャッシュデータM1をデジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化し、

$$Cm1ks2 = E(Ks2, M1)$$

通信ネットワーク8を介して暗号化デジタルキャッシュデータCm1ks2を小売店38の電子財布であるユーザ端末装置に転送することにより、支払を行う。このとき

に、顧客情報Icも小売店38のユーザ端末装置に転送される。また、残額デジタルキャッシュデータM2はデジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化され、

$$Cm2ks2 = E(Ks2, M2)$$

顧客36のユーザ端末装置内に保存される。

【0250】暗号化デジタルキャッシュデータCmlks2及び顧客情報Icを転送された小売店38は、転送された暗号化デジタルキャッシュデータCmlks2及び顧客情報Icをユーザ端末装置に保存するとともに、内容を10 確認するために通信ネットワーク8を経由して小売店側銀行39に顧客情報Icを提示して、復号鍵である第2秘密鍵Ks2の転送を依頼する。小売店38から第2秘密鍵Ks2の転送依頼を受けた小売店側銀行39は、第2秘密鍵Ks2の転送依頼とともに顧客情報Icを顧客側銀行37に転送する。小売店側銀行39から第2秘密鍵Ks2の転送依頼を転送された顧客側銀行37は、第2秘密鍵Ks2が顧客情報Icのみに基づいている場合にはデジタルキャッシュ管理プログラムPにより顧客情報Icに基づいて第2秘密鍵Ks2を生成し、第2秘密鍵Ks2が顧20 客情報Icと第1秘密鍵Ks1に基づいている場合にはデジタルキャッシュ管理プログラムPにより顧客情報Icと第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、生成された第2秘密鍵Ks2を小売店側銀行39に転送する。顧客側銀行37から第2秘密鍵Ks2を転送された小売店側銀行39は、通信ネットワーク8を経由して第2秘密鍵Ks2を小売店38に転送する。

【0251】第2秘密鍵Ks2を転送された小売店38は、デジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化デジタルキャッシュデータ30 Cm1ks2を復号化し、

$$M1 = D(Ks2, Cm1ks2)$$

金額を確認の上、商品を顧客36に発送する。なお、この場合小売店36が小売店側銀行39ではなく顧客側銀行37に直接に第2秘密鍵Ks2の転送を依頼するようにすることもできる。

【0252】小売店38が収受したデジタルキャッシュを小売店側銀行39の口座に入金する場合には、通信ネットワーク8を経由して小売店側銀行39に暗号化デジタルキャッシュデータCmlks2とともに顧客情報Ic40 を転送する。暗号化デジタルキャッシュデータCmlks2と顧客情報Icを転送された小売店側銀行39は、顧客情報Icを転送することにより第2秘密鍵Ks2の転送を顧客側銀行24に対して依頼する。小売店側銀行39から第2秘密鍵Ks2の転送を依頼された顧客側銀行37は、第2秘密鍵Ks2が顧客情報Icのみに基づいている場合にはデジタルキャッシュ管理プログラムPにより顧客情報Icに基づいて第2秘密鍵Ks2を生成し、第2秘密鍵Ks2が顧客情報Icと第1秘密鍵Ks1に基づいて50 いる場合にはデジタルキャッシュ管理プログラムPに

より顧客情報Icと第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、生成された第2秘密鍵Ks2を小売店側銀行39に転送する。顧客側銀行37から第2秘密鍵Ks2を転送された小売店側銀行39は、デジタルキャッシュ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化デジタルキャッシュデータCmlks2を復号化し、

$$M1 = D(Ks2, Cm1ks2)$$
 復号化デジタルキャッシュデータM1を小売店39の銀行口座に入金する。

【0253】一般的な取引システムにおいては、小売店38はメーカ40あるいはメーカ40と小売店38の間に介在する卸売り店から商品を仕入れ、顧客36に販売する。そのため、顧客36と小売店38との間に存在するのと同様の取引形態が小売店38とメーカ40との間にも存在する。この小売店38とメーカ40との間で行われるデジタルキャッシュの取り扱いは、顧客36と小売店38との間で行われるデジタルキャッシュの取り扱いと基本的な相違はないため、煩雑さをさけるため説明を省略する。

【0254】このデジタルキャッシュシステムにおける、デジタルキャッシュの取扱いはすべて銀行を介在させて行われるため、顧客側銀行にデジタルキャッシュの取扱いに関する金額、日付、秘密鍵要求者情報等の情報を保存しておくことにより、デジタルキャッシュの残高及び使用履歴を把握することができる。また、デジタルキャッシュデータを保存する電子財布であるユーザ端末装置が紛失あるいは破損により使用不能となった場合でも、顧客側銀行に保存されている使用残高及び使用履歴に基づきデジタルキャッシュを再発行することが可能である。なお、デジタルキャッシュの安全性を高めるためにデジタルキャッシュデータにデジタル署名を付けることが望ましい。この実施例において、デジタルキャッシュには顧客情報が付加されており、この顧客情報はデジタル署名付とされることがある。つまり、この実施例においてデジタルキャッシュは顧客を振り出し人とする手形決済システムとしての機能も有する。さらに、このシステムは従来紙を用いて行われている国際貿易における信用状、船積み有価証券等による各種決済システムにも応用することができる。

【0255】【実施例18】実施例17で説明したデジタルキャッシュシステムにおけるデジタルキャッシュの取扱いはすべて銀行を介在させて行われるが、この他に銀行を介在させることなくデジタルキャッシュを取り扱うこともできるので、次に、銀行を介在させないデジタルキャッシュシステムを説明する。このデジタルキャッシュシステムにおいては、デジタルキャッシュデータを暗号化する暗号鍵として公開鍵及び専用鍵が用いられ、実施例17で用いられる秘密鍵Ks及び顧客情報Icは用いられない。したがって、この実施例に50 おいてデジタルキャッシュは貨幣と同様な形態で使用

される。これら以外の点は、実施例17のシステム構成と異なる点はないので具体的な説明は省略する。

【0256】このデジタルキャッシュシステムに関係する各銀行、顧客、小売店、メーカでデジタルキャッシュを受け取る側になる者は、各々公開鍵及び専用鍵を用意する。その中の公開鍵は支払予定者に予め送付しておくことも、あるいは取引を行う前に支払者に送付することもできるが、ここでは支払予定者に予め配布されているものとして説明する。顧客36は端末装置を利用して通信ネットワーク8を経由して金額を指定することにより、顧客側銀行37に預金口座からの預金の引出の申込を行う。顧客36から預金引出の申込を受けた顧客側銀行37は、引出金額のデジタルキャッシュデータM0を予め送付されている顧客公開鍵Kbcを用いてデジタルキャッシュ管理プログラムPにより暗号化し、 $Cm0kbc = E(Kbc, M0)$

暗号化デジタルキャッシュデータCm0kbcを顧客36に転送する。

【0257】暗号化デジタルキャッシュデータCm0kbcを転送された顧客36は、デジタルキャッシュ管理プログラムPにより顧客公開鍵Kbcに対応する顧客専用鍵Kvcを用いて復号化し、 $M0 = D(Kvc, Cm0kbc)$

内容を確認し、端末装置内に残金額のデータM1がある場合には残金額のデータをM2 ($= M0 + M1$) に変更し、金額が変更されたデジタルキャッシュデータM2をデジタルキャッシュ管理プログラムPにより顧客公開鍵Kbcで暗号化して、 $Cm2kbc = E(Kbc, M2)$

端末装置内に保存する。

【0258】小売店38から物品の購入を希望する顧客36は、端末装置に保存されている暗号化デジタルキャッシュデータCm2kbcをデジタルキャッシュ管理プログラムPにより顧客専用鍵Kvcを用いて復号化し、 $M2 = D(Kvc, Cm2kbc)$

必要な金額に対応するデジタルキャッシュデータM3を予め送付されている小売店公開鍵Kbsを用いてデジタルキャッシュ管理プログラムPにより暗号化し、 $Cm3kbs = E(Kbs, M3)$

通信ネットワーク8を介して小売店38の端末装置に転送することにより、支払を行う。また、残額デジタルキャッシュデータM4 ($= M2 - M3$) はデジタルキャッシュ管理プログラムPにより顧客公開鍵Kbcで暗号化されて、 $Cm4kbc = E(Kbc, M4)$

端末装置内に保存される。

【0259】暗号化デジタルキャッシュデータCm3kbsを転送された小売店38は、デジタルキャッシュ管理プログラムPにより小売店公開鍵Kbsに対応する小売店専用鍵Kvsを用いて復号化し、

$M3 = D(Kvs, Cm3kbs)$

内容を確認し、端末装置内に残金額のデータM5がある場合には残金額のデータをM6 ($= M5 + M3$) に変更し、金額が変更されたデジタルキャッシュデータM6をデジタルキャッシュ管理プログラムPにより小売店公開鍵Kbsで暗号化して、 $Cm6kbs = E(Kbs, M6)$ 端末装置内に保存する。

【0260】メーカ40に対する商品仕入代金の決済を行うおうとする小売店38も同様な方法で決済を行う。さらには、顧客36の顧客側銀行37への入金、小売店36の小売店側銀行39への入金、メーカ40のメーカ側銀行41への入金も同様な方法で行われる。

【0261】以上説明した実施例17及び実施例18においては、デジタルキャッシュシステムを実現するために図4を用いて説明されたデータ著作権管理システムの構成を応用し、さらに実施例17においては顧客情報を利用し、用いられる秘密鍵を変化させ、実施例18においては公開鍵及び専用鍵を用いている。しかし、デジタルキャッシュシステムを実現させるシステムの構成として、この他の著作権管理システムの構成すなわち、図1に示されたデータ著作権管理システム、図2に示されたデータ著作権管理システム、図3に示されたデータ著作権システム、図5に示されたデータ著作権システムの何れの構成も応用可能である。また、その場合に用いられる暗号鍵方式としては、変化しない秘密鍵、公開鍵と専用鍵、秘密鍵と公開鍵と専用鍵の組み合わせ、鍵の2重化、という実施例1から実施例13で説明した暗号鍵方式の何れもが応用可能である。

【0262】【実施例19】これまでは従来の音声電話器にテレビジョン映像を付加したものに過ぎなかったテレビジョン会議システムが、最近ではコンピュータシステムに組み込まれることにより音声あるいは映像の品質が向上したばかりでなく、コンピュータ上のデータも音声及び映像と同時に扱うことができるように進化している。このような中で、テレビジョン会議参加者以外の監視による使用者のプライバシー侵害及びデータの漏洩に対するセキュリティは秘密鍵を用いた暗号化システムによって保護されている。しかし、テレビジョン会議参加者自身が入手する会議内容は復号化されたものであるため、テレビジョン会議参加者自身が会議内容を保存し、場合によっては加工を行い、さらにはテレビジョン会議参加者以外の者に配布する2次的な利用が行われた場合には他のテレビジョン会議参加者のプライバシー及びデータのセキュリティは全く無防備である。特に、伝送データの圧縮技術が発達する一方でデータ蓄積媒体の大容量化が進んだ結果テレビジョン会議の内容全てがデータ蓄積媒体に複写されたりあるいはネットワークを介して転送される恐れさえ現実のものとなりつつある。

【0263】この実施例はこのような状況に鑑みて、こ

れまでに説明したデータ著作権管理システムの構成をテレビジョン会議システムに応用することにより、テレビジョン会議参加者自身の二次的な利用による他のテレビジョン会議参加者のプライバシー及びデータのセキュリティ確保を行うものである。

【0264】このテレビジョン会議データ管理システムは、例えば図4に示されたデータ著作権管理システムの構成におけるデータベース1をテレビジョン会議第1参加者に、1次ユーザ端末装置4をテレビジョン会議第2参加者に、2次ユーザ端末装置5をテレビジョン会議非参加者に置き換えることにより実現することができる。この実施例を図9を用いて説明する。この図において、44はテレビジョン会議第1参加者、45はテレビジョン会議第2参加者、46はテレビジョン会議第3非参加者及び47はテレビジョン会議第4非参加者、8は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCAテレビジョン回線等の通信ネットワークであり、テレビジョン会議第1参加者44とテレビジョン会議第2参加者45は通信ネットワーク8によって相互に接続可能とされている。また、テレビジョン会議第2参加者45とテレビジョン会議第3非参加者46、テレビジョン会議第3非参加者46とテレビジョン会議第4非参加者47は通信ネットワーク8で接続可能とされている。また、48はデータ記録媒体である。この図において、破線で示されたのは暗号化されたテレビジョン会議内容の経路であり、実線で示されたのはテレビジョン会議第3非参加者46及びテレビジョン会議第4非参加者47からテレビジョン会議第1参加者へ暗号鍵を要求する経路であり、1点鎖線で示されたのはテレビジョン会議第1参加者44からテレビジョン会議第2参加者45、テレビジョン会議第3非参加者46及びテレビジョン会議第4非参加者47へ暗号鍵が転送される経路である。なお、この実施例で説明するテレビジョン会議データ管理システムでは説明を簡明にするために、テレビジョン会議第1参加者44のプライバシー及びデータセキュリティの確保のみが行われる場合について説明するが、テレビジョン会議第2参加者45のプライバシー及びデータセキュリティの確保も行うことが可能であることはいうまでもない。

【0265】映像及び音声を含むテレビジョン会議第1参加者44のテレビジョン会議データを暗号化／復号化するテレビジョン会議管理プログラムPはテレビジョン会議第2参加者45、テレビジョン会議第3非参加者46及びテレビジョン会議第4非参加者47に予め配布され、各々の端末装置に内蔵されている。なお、テレビジョン会議データ管理プログラムPは暗号鍵が転送される毎に転送されるようにすることもできる。さらに、この実施例では暗号鍵としてテレビジョン会議第1参加者44が用意する第1秘密鍵及びテレビジョン会議第2参加者45が生成する第2秘密鍵、テレビジョン会議第3非

参加者46が生成する第3秘密鍵・・・が用いられる。

【0266】テレビジョン会議第1参加者44とテレビジョン会議第2参加者45は、各端末装置を利用し、通信ネットワーク8を経由して音声、映像、データ（これらを一括して「テレビジョン会議データ」と呼ぶ）を相互に転送することによりテレビジョン会議を行うが、テレビジョン会議を開始する前にテレビジョン会議第1参加者44は第1秘密鍵Ks1を選択あるいは生成し、第1秘密鍵Ks1をテレビジョン会議を開始する前にテレビジョン会議第2参加者45に供給する。また、第1秘密鍵Ks1を転送されたテレビジョン会議第2参加者45は、テレビジョン会議データ管理プログラムPにより、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、 $Ks2 = P(Ks1)$ 生成された第2秘密鍵Ks2を端末装置内に保存しておく。

【0267】テレビジョン会議第1参加者44は、通信ネットワーク8を経由して行われるテレビジョン会議において、テレビジョン会議データM0を第1秘密鍵Ks1で暗号化し、

$$Cm0ks1 = E(Ks1, M0)$$

暗号化されたテレビジョン会議データCm0ks1をテレビジョン会議第2参加者45に転送する。

【0268】第1秘密鍵Ks1を用いて暗号化されたテレビジョン会議データCm0ks1を受け取ったテレビジョン会議第2参加者45は、第1秘密鍵Ks1を用いて暗号化されたテレビジョン会議データCm0ks1を復号し、

$$M0 = D(Ks1, Cm0ks1)$$

復号化されたテレビジョン会議データM0を利用する。

また、テレビジョン会議データ管理プログラムPにより、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2が生成される。

$$Ks2 = P(Ks1)$$

【0269】復号されたテレビジョン会議データM0がテレビジョン会議第2参加者45の端末装置内に保存される場合、データ記録媒体48に複写される場合、通信ネットワーク8を経由してテレビジョン会議第3非参加者に転送される場合には、そのデータMはテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0270】暗号化データCmks2は、テレビジョン会議データ名あるいはテレビジョン会議データ番号とともに、記録媒体11に複写され、あるいは、通信ネットワーク8を経由してテレビジョン会議第3非参加者に供給される。

【0271】暗号化データCmks2を入手したテレビジョン会議第3非参加者46は端末装置を利用して、テレビジョン会議データ名あるいはテレビジョン会議データ番号を指定することによりテレビジョン会議データMの2

次利用をテレビジョン会議第1参加者44に申し込む。

【0272】データMの2次利用申込を受けたテレビジョン会議第1参加者44は、テレビジョン会議データ名あるいはテレビジョン会議データ番号を手がかりとして第1秘密鍵Ks1を探し出し、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、

$$Ks2 = P(Ks1)$$

生成された第2秘密鍵Ks2をテレビジョン会議第3非参加者46に供給する。

【0273】第2秘密鍵Ks2を受け取ったテレビジョン会議第3非参加者46は、暗号化データCmks2をテレビジョン会議データ管理プログラムPを利用して第2秘密鍵Ks2を用いて復号化して

$$M = D(Ks2, Cmks2)$$

復号化されたテレビジョン会議データMを利用する。テレビジョン会議データMがテレビジョン会議第3非参加者46の端末装置内に保存される場合、記録媒体49に複写される場合、通信ネットワーク8を経由してテレビジョン会議第4非参加者47に転送される場合には、そのテレビジョン会議データMはテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。

$$Cmks2 = E(Ks2, M)$$

【0274】なお、さらにテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2に基づいて第3秘密鍵Ks3が生成され、

$$Ks3 = P(Ks2)$$

テレビジョン会議データ管理プログラムPによりこの生成された第3秘密鍵Ks3を用いてデータMが暗号化されるようにすることもできる。

$$Cmks3 = E(Ks3, M)$$

【0275】以上説明した実施例19においては、テレビジョン会議データ管理システムを実現するために図4を用いて説明されたデータ著作権管理システムの構成を応用し、使用される秘密鍵を変化させている。しかし、テレビジョン会議データシステムを実現させるシステムの構成として、この他のシステム構成すなわち、図1に示されたシステム構成、図2に示されたシステム構成、図3に示されたシステム構成、図4に示されたシステム構成の何れもが応用可能である。また、その場合に用いられる暗号鍵方式としては、変化しない秘密鍵、公開鍵と専用鍵、秘密鍵と公開鍵と専用鍵の組み合わせ、鍵の2重化、という実施例1から実施例13で説明した暗号鍵方式が応用可能である。

【0276】また、この説明ではテレビジョン会議第2参加者がテレビジョン会議データを保存して利用すること及び記録媒体に複写あるいは通信ネットワークを経由して転送することを前提にしているが、暗号化に使用された暗号鍵が直ちに廃棄されるようにすることにより、

これらの行為を制限することもできる。

【0277】【実施例20】前に説明したように、本発明のシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要があり、また、この登録の際にデータベース用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に第1暗号鍵を用いた著作権管理プログラムを復号するためのプログラムが含まれているため、その保護を図る必要がある。また、本発明においてはデータMを利用するために第1暗号鍵K1、第2暗号鍵K2及び著作権管理プログラムPが各ユーザに対して転送され、各ユーザはこれらを保管しておく必要がある。さらには著作権情報ラベル、ユーザ情報、公開鍵方式の公開鍵と専用鍵そして秘密鍵生成アルゴリズムを含むプログラム等が必要に応じて保管される。

【0278】これらを保管しておく手段としてフレキシブルディスクを使用することが最も簡便な手段であるが、フレキシブルディスクはデータの消失あるいは改竄に対して極めて脆弱である。また、ハードディスクドライブを使用した場合にもフレキシブルディスク程ではないがデータの消失あるいは改竄に対する不安がある。ところで、最近カード形状の容器にIC素子を封入したICカードが普及し、特にマイクロプロセッサを封入したPCカードがPCMCIAカードあるいはJEIDAカードとして規格化が進められている。

【0279】図10に示されたのは、このPCカードを用いて本発明のデータベース著作権管理システムのユーザ端末装置を構成した実施例である。この図において、50はユーザ端末装置本体のマイクロプロセッサであり、51はシステムバスである。また、52は内部にPCカードマイクロプロセッサ53、読み出し専用メモリ55、書き込み・読み出しメモリ56が封入されこれらがPCカードマイクロプロセッサバス54で接続されたPCカードである。

【0280】読み出し専用メモリ55には、データベース用ソフトウェア及びユーザデータ等の固定した情報がデータベース組織において格納されている。また、この読み出し専用メモリ55には鍵管理センタ9あるいは著作権管理センタから供給される第1暗号鍵、第2暗号鍵及び著作権管理プログラムも格納される。この読み出し専用メモリ55は書き込みも行われるため、EEPROMを使用することが最も簡便である。

【0281】前に説明したように、データ、第1暗号鍵K1、第2暗号鍵K2、第3暗号鍵K3・・・及び著作権管理プログラムP1、P2、P3・・・はいずれも暗号化された状態でユーザに供給され、データを利用するには第1暗号鍵K1、著作権管理プログラムP、データM及び第2暗号鍵K2を復号しなければならない。これらの作業はユーザ端末装置本体のマイクロプロセッサ50がPCカード52の読み出し専用メモリ55に格納され

ているソフトウェア。第1暗号鍵K1及び著作権管理プログラムP1を用いて行ってもよいが、その場合にはこれらのデータがユーザ端末装置に転送されるため、不正規な使用が行われる危険性がある。この危険を避けるためにはすべての作業をPCカード52内のマイクロプロセッサ53がCPUバス54を介して書き込み・読み出しメモリ56を利用して行い、結果だけをユーザ端末装置に転送し各種の利用を行うようにする。このPCカードを利用した場合には異なる装置をユーザ端末装置とすることができる。また、PCカードの他にこれらの機能

を有するボードあるいは外部装置を用いることもできる。

【図面の簡単な説明】

【図1】 本発明実施例1、実施例2、実施例3のデータ著作権管理システム構成図。

【図2】 本発明実施例4のデータ著作権管理システム構成図。

【図3】 本発明実施例5、実施例6、実施例7のデータ著作権管理システム構成図。

【図4】 本発明実施例8、実施例9、実施例10、実施例11のデータ著作権管理システム構成図。

【図5】 本発明実施例12、実施例13のデータ著作権管理システムの実施例。

【図6】 データ加工の説明図。

【図7】 デジタルキャッシュシステムの説明図。

【図8】 本発明実施例17、実施例18のデジタルキャッシュシステム構成図。

【図9】 本発明実施例19のテレビジョン会議システム構成図。

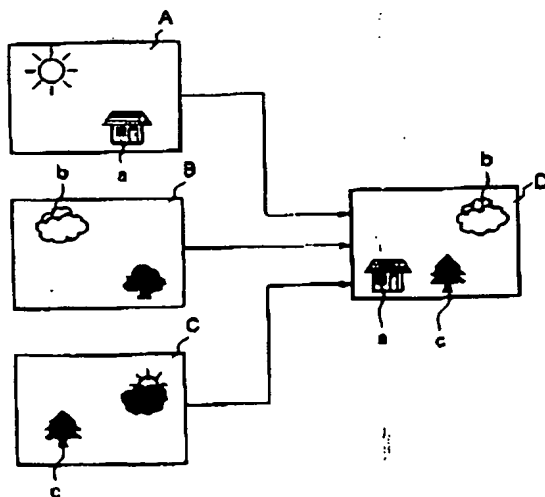
【図10】 本発明のデータ著作権管理システムで用い

るユーザ端末装置の実施例構成図。

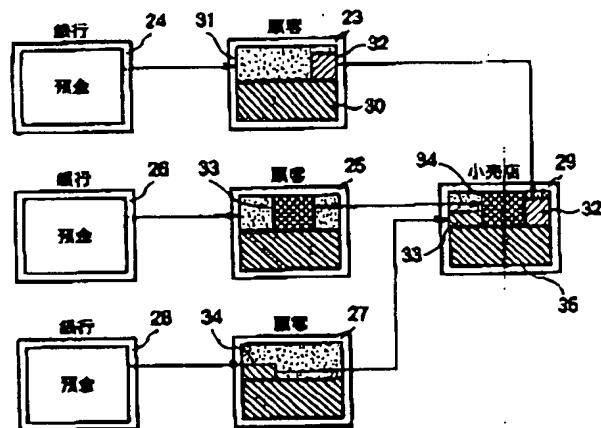
【符号の説明】

1. 19, 20, 21 データベース
- 2 放送・通信衛星
- 3 11, 12, 13, 48, 49 記録媒体
- 4, 5, 6, 7 ユーザ端末装置
- 8 通信ネットワーク
- 9 鍵管理センタ
- 10, 14, 15, 17, 18 著作権管理センタ
- 23, 25, 27, 29 電子財布
- 24, 26, 28 預金口座
- 30, 35 残金
- 31 引出金
- 32, 33, 34 支払金
- 36 顧客
- 38 小売店
- 40 メーカ
- 37 顧客側銀行
- 39 小売店側銀行
- 41 メーカ側銀行
- 42, 43 ICカード
- 44, 45 テレビジョン会議参加者
- 46, 47 テレビジョン会議非参加者
- 50 マイクロプロセッサ
- 51 システムバス
- 52 PCカード
- 53 PCカードマイクロプロセッサ
- 54 PCカードマイクロプロセッサバス
- 55 読み出し専用メモリ
- 56 書き込み・読み出しメモリ

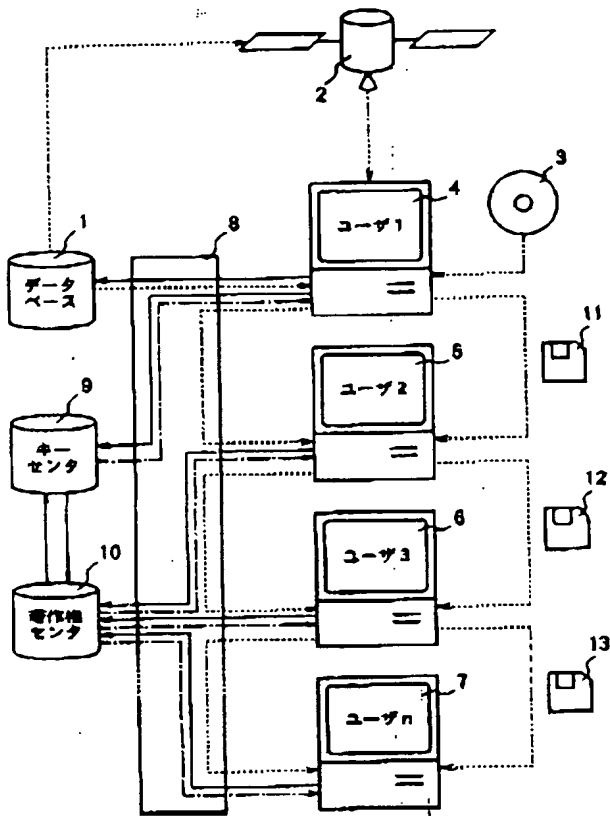
【図6】



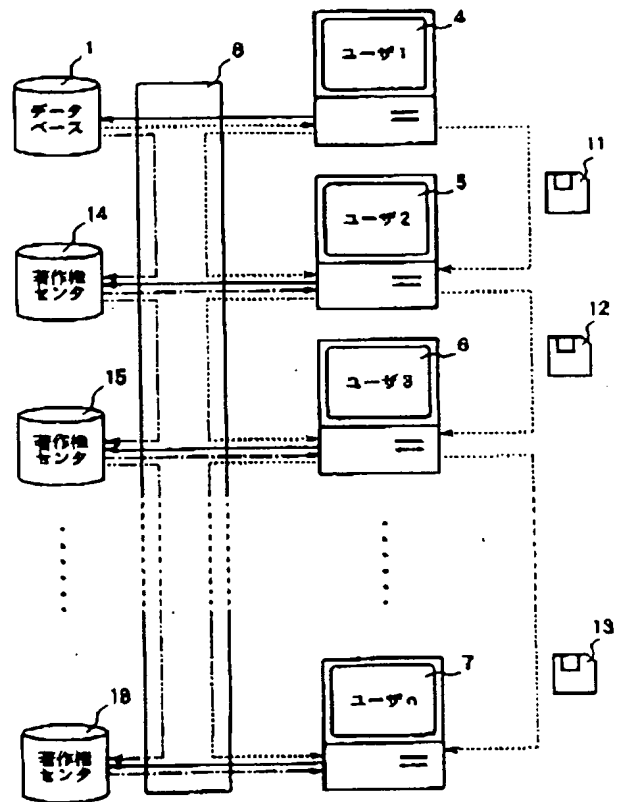
【図7】



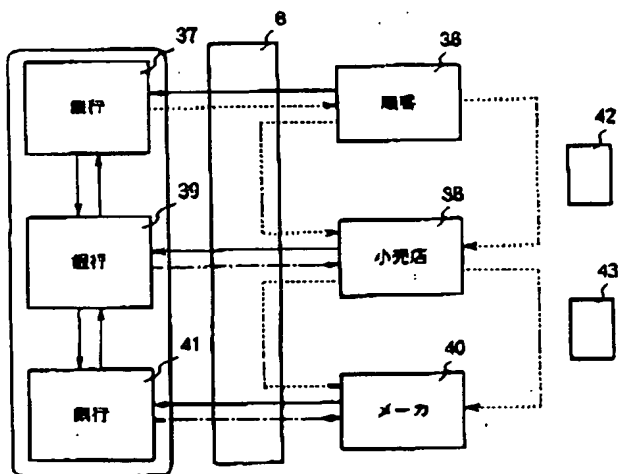
【図1】



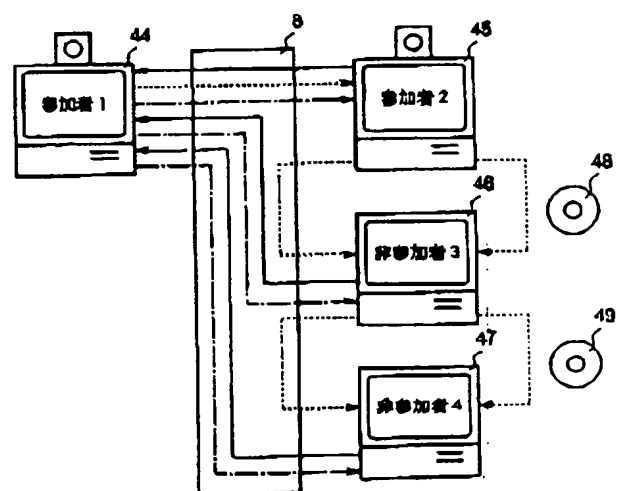
【図2】



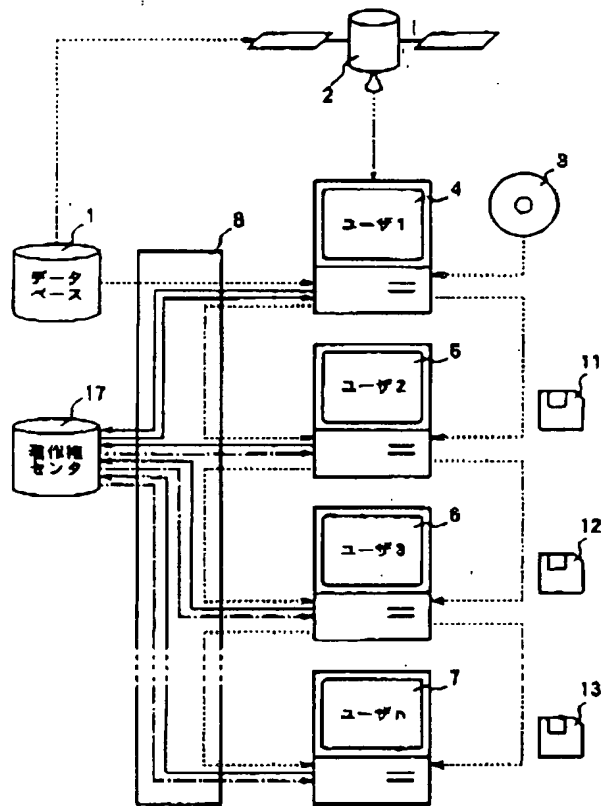
【図8】



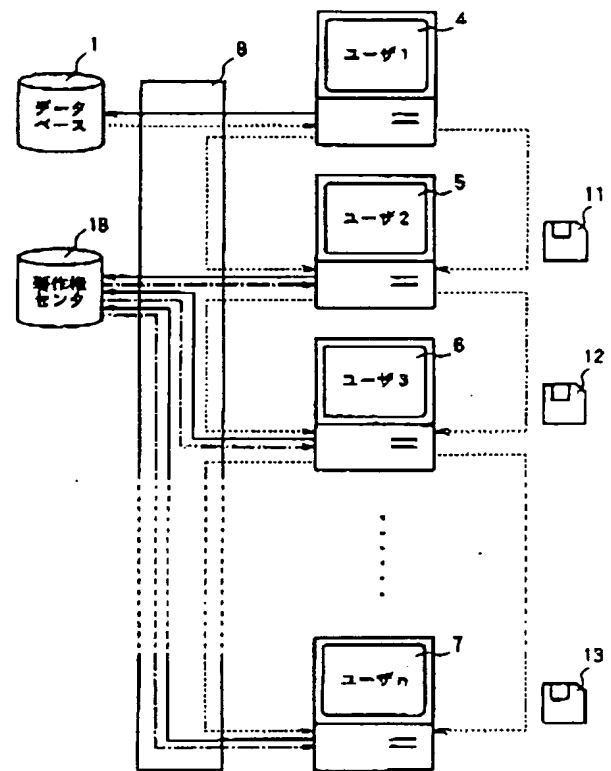
【図9】



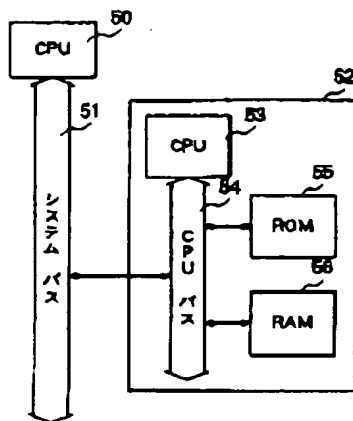
【図3】



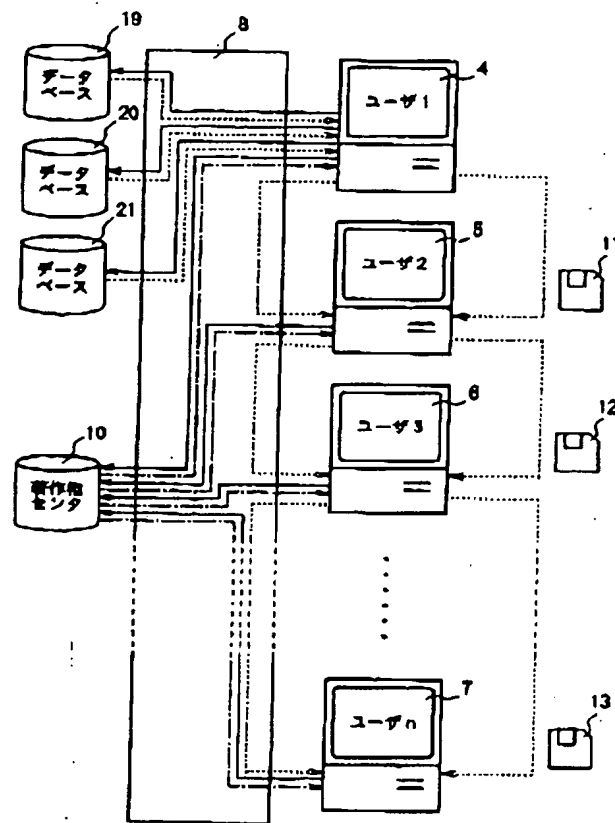
【図4】



【図10】



【図5】



フロントページの続き

(51) Int. Cl. 6

H04L 9/00

9/10

9/12

識別記号

庁内整理番号

F I

技術表示箇所